BRIEF CONTENTS

Part I—Getting Started

1 Getting Started 1

Part II—Administering the System

2 System Settings 29
3 Administering the Domain 83
4 Trunks 113
5 Dial Plans 147
6 Extensions 161
7 Park Orbits 177
8 Service Flags 181
9 Auto Attendant 193
10 Hunt Groups 215
11 Agent Groups 225
12 Paging 251
13 Conferencing 259
14 IVR Node 271
15 Calling Card Account 283
16 Pre-Pay Feature 289
17 Email 295
18 Audio and Greetings 309
19 Buttons 327
20 Plug and Play 343
21 Music on Hold 379
22 Call Detail Records (CDRs) 393

Part III—The User Interface

23 Web Interface 403
24 Star Codes 429
25 Voicemail 451
26 Cell Phones 463

Appendix A. Working with CSV Files 479
Appendix B. SIP Overview 503
Appendix C. snom ONE and Exchange 531

Glossary 539

Index 559

CONTENTS

Part I—Getting Started

1 Getting Started **1**

About snom ONE 1

Memory/Hardware Requirements 2

USB Device 4

Warnings 4

Standards Conformance 4

Disposal 4

Installing the Software 5

Windows Installations 5

MAC OS Installations 7

Linux Installations 10

Upgrading the Software 14

Manual Software Upgrades (Windows) 15

Mac OS Upgrades 16

Linux Upgrades 17

Logging In 18

Login Levels 19

Activating Your License 21

Restarting the System 21

Restarting From Windows (Service Control Manager) 22

Restarting From a Command Line 23

Restarting From Mac OS 23

Restarting From a Linux Environment 23

Manually Starting the Service 23

When the System Fails to Restart 24

Technical Support 25

Documentation .....

Part II—Administering the System

2 System Settings **29**

Directory Structure 33

Directory Tree 33
Global Configuration File 34
Folder Overview 35
Folder Details 37
Configuring System Settings 42
General 42
Administrator Login 44
Appearance 45
Performance 48
SIP Settings 51
Ports 53
HTTP Ports 53
SIP Ports 54
RTP Ports 56
SNMP 58
TFTP 59
LDAP 60
Logging 60
General Logging 61
Specific Events 62
SIP Logging 63
Configuration 66
Save/Restore a Backup 66
Request Configuration 67
Reload Configuration Files 67
Schedule a Reboot 68
Certificates 69
Access List 71
Web Page Control 74
Templates 74
Translation 77
User Page Control 78

3 Administering the Domain 83
Naming the Domain 84
Changing the Name of the Domain 84
Assigning a Domain Administrator 85
Domains—Default and New 89
Default Domain 89

Creating New Domains ... 90
Configuring the Domain ... 93
Accounts Page Display ... 101
Recording Defaults ... 104
Email Settings ... 104
Midnight Events ... 105
Domain Address Book ... 108
Creating a Domain Address Book ... 109
Searching for Contacts ... 111

4 Trunks ... 113
Trunk Types ... 114
SIP Registrations ... 114
SIP Gateway ... 116
Outbound Proxy ... 116
Inbounds Calls ... 117
How the System Identifies a Trunk ... 117
How the System Routes a Call to the Proper Extension ... 119
Basic Routing ... 119
When Regular Expressions are Involved ... 121
Regular Expressions and Direct Inward Dialing (DID) ... 124
Outbound Calls ... 127
Caller-ID ... 127
Generating the ANI ... 128
Representing the Source ... 129
Creating Trunks ... 130
Configuring Trunks ... 131
General Settings ... 131
Outbound Settings ... 139
Inbound Settings ... 141
Connecting Branch Offices Together ... 142
Using a Gateway Trunk ... 142
Using a SIP Registrations Trunk (SIP Tie Line) ... 144

5 Dial Plans ... 147
Parts of a Dial Plan ... 148
Key Components ... 148
Wildcard Patterns ... 151
Regular Expression Matching ... 152

Building a Dial Plan ... 153
Creating a Dial Plan ... 153
Configuring the Dial Plan ... 153
Sample Dial Plans ... 155
Typical Dial Plan ... 155
A Simplified Dial Plan ... 156
Dial Plan with Prefix in Front of the Number ... 156
A North American Dial Plan ... 156
Sending Star Codes on a Trunk ... 157
Forced Matching ... 158
Inter-Domain Dialing ... 158
Domains with Non-Overlapping Extensions ... 159
Domains with Overlapping Extensions ... 159

6 Extensions ... 161
Preparing the User Account ... 162
Working with Default Extensions ... 162
Importing Multiple Extensions (Bulk) ... 164
Creating a Few New Extensions ... 164
Before Registering the Extension ... 167
Administrator-Only Settings ... 167
Registration Settings ... 169
Permission Settings ... 173

7 Park Orbits ... 177
Creating a Park Orbit ... 178
How the Park Orbit Works ... 180
Parking Calls ... 180
Retrieving Calls ... 180
Using a Park Orbit Button ... 180

8 Service Flags ... 181
Setting up a Service Flag Account ... 183
Linking a Service Flag to an Account ... 186
Method 1: Night Service ... 186
Method 2: Message-Only and Voicemail Options ... 188
Setting/Clearing a Service Flag ... 190
Setting a Manual Service Flag from the Phone ... 190
Setting a Manual Service Flag from the Web Interface ... 191

Service Flags and Buttons ... 191
Using a Button to Activate a Service Flag ... 191

9 Auto Attendant ... 193
How an Auto Attendant Works ... 196
Welcome Message ... 196
Processing User Input ... 196
Ringing an Extension ... 197
Blacklisted Callers and Anonymous Calls ... 198
Multiple Messages—Time-Based Configuration ... 198
Setting up an Auto Attendant ... 198
Auto Attendant Behavior ... 199
Timeout Handling ... 203
Night Service ... 204
Dial-by-Name ... 205
Direct Destinations ... 205
Nesting Auto Attendants ... 207
Welcome Greetings ... 209
Overview ... 209
Recording the Greeting ... 209
Filing System and Naming Conventions ... 211

10 Hunt Groups ... 215
How the Hunt Group Works ... 217
Setting up a Hunt Group ... 218
Identity ... 219
Ring Stages ... 220
Behavior ... 221
Night Service ... 223

11 Agent Groups ... 225
How the Agent Group Works ... 227
The Message-Music Cycle ... 227
Setting up an Agent Group Account ... 229
Identity ... 230
Behavior ... 231
Connecting Caller to Agent ... 238
Preventing Lengthy Periods in Ringback or Queue ... 239
Mapping Telephone Keypad Numbers with Extensions ... 240

Night Service ... 242
SOAP Interface ... 243
Logging In and Out ... 244
Method 1: Buttons ... 244
Method 2: Star Codes ... 245
Monitoring Agent Groups ... 246
Monitoring from the Web Interface ... 246
Monitoring Using Buttons on Phone ... 248
Monitoring from the WAC (Web-Based Console) ... 248

12 Paging ... 251
Types of Paging ... 251
Unicast Paging ... 251
Multicast Paging ... 252
Setting up a Paging Account ... 253
Assigning Multicast IP Addresses to IP Phones ... 257

13 Conferencing ... 259
Scheduled Conferences ... 261
Creating a Scheduled Conference Account ... 261
Scheduling a New Conference ... 263
Modifying Scheduled Conferences ... 265
Moderating Scheduled Conferences ... 265
Ad Hoc Conferences ... 266
Creating an Ad Hoc Conference Account ... 266
Calling into an Ad Hoc Conference ... 268
Moderating an Ad Hoc Conference ... 269

14 IVR Node ... 271
How the IVR Node Works ... 272
Setting up an IVR Node Account ... 274
Identity ... 275
Settings ... 276
Recording Messages ... 277
Record the Message Directly ... 277
Upload a WAV File ... 278
Linking an External Application Server to an IVR Node ... 279
Sample SOAP Message ... 279

15 Calling Card Account 283
Setting up a Calling Card Account 284
Identity 285
Behavior 286

16 Pre-Pay Feature 289
Setting up the Pre-Pay 290
Creating the Rates Table 290
Assigning a Dollar Amount to an Extension 292
Methods of Access 293
Extension 293
Personal Virtual Assistant 293
Calling Card Account (PIN Access) 294

17 Email 295
Configuring the SMTP Server 295
System-Wide SMTP Settings 295
Adding Email Accounts to the System 299
Receiving Email Notifications from the System 303
Types of Email Notifications 303
CDRs to Email 304
CDRs for Trunk Activity 304
CDRs for Your Extension Only 305
CDRs for All Extensions on Your Domain 306
CDRs for All Extensions on All Domains 306
Call Recording to Email 307
Blacklist Activity to Email 307
System-Initiated 307

18 Audio and Greetings 309
Greetings 309
Personal Greetings 309
Auto Attendant Greetings 311
Agent Group Greetings 313
Recorded Phone Calls 315
User-Initiated Recordings 316
System-Initiated Recordings 317
File System 317
Notes 320

Audio Prompts 321
Uploading New Languages 322
Customized Ringtones 323

19 Buttons 327
Creating a Button Profile 331
Point-and-Click Method 331
CSV Method 334
Assigning Button Profiles to Users 336
Assigning a Profile to a Single User 336
Massive Update of Profiles 336
Key System Configuration 338
Setting up a Key System 338
Multiple Identities and Button Profiles 341

20 Plug and Play 343
Finding the snom ONE 343
Plug and Play Checklist 345
Configuring the Administrator Settings 345
Configuring the Domain Settings 346
Creating an Authentication Password 348
Setting up the Domain Address Book 349
Configuring the Button Profiles 349
Creating the Extension(s) 349
Performing Plug and Play 352
DHCP, Option 66 352
SIP SUBSCRIBE (Multicast) 353
Mass Deployment 354
Manual Method (HTTP) 355
Resetting the Phone 359
Using the Phone 359
Rebooting the Phone 361
Using the Phone 361
Using the Phone GUI 361
Updating the Firmware Via TFTP 362
Download the Recovery Firmware 362
TFTP Process 364
Registering Numerous Extensions to One Phone 365
Overriding Plug and Play Defaults 367

Changing Default Settings from Admin > Settings > PnP 367
Changing Default Settings Using a Customized XML File 369
Troubleshooting .....

21 Music on Hold 375
Setting up Music on Hold 376
Editing MoH Sources 378
Creating WAV Files 379
Configuring Paging/Music on Hold 381
Download and Installation 381
Setting up Paging 382
Configuring Music on Hold 385
XML Configuration File 387

22 Call Detail Records (CDRs) 389
CDRs for Third-Party Software Vendors 390
CDR to CSV 391
CDR to Email 392
CDR to Simple TCP 392
CDR to SOAP/XML 395

Part III—The User Interface

23 Web Interface 399
Logging in 399
Extension Settings 401
General Settings 402
Redirection Settings 406
Email Settings 411
Instant Message 414
Call Lists 415
Mailbox 415
Missed Calls 415
Call Log 416
Contacts 418
Personal Address Book 418
Domain Address Book 422
Upload Domain Address Book to Phone 423

Extension Status 423

24 Star Codes 425
Basic Star Codes 427
Redial a Number (*66) 427
Call Return (*69) 427
Intercom (*90) 427
Transferring Calls 428
Transfer Calls 428
Transfer a Call Directly to Someone's Voicemail 429
Call Park (*85) and Call Park Retrieve (*86) 430
Call Pickup (*87) 431
Conferencing 433
Three-Way Conferences 433
Conference (*53) 433
Anonymous Calls 434
Block Caller-ID (*67) 434
Reject Anonymous Calls (*88) 435
Forwarding Calls 435
Hot Desking (*70) 435
Call Forward All Calls (*71/*72) 437
Call Forward on Busy (*73/*74) 437
Call Forward on No Answer (*75/*76) 438
Do Not Disturb (*78) 439
Set Night Mode for Domain Accounts (*80) 439
Call Center Features 440
Agent Log in/Log out (*64/*65) 441
Call Barge (*81) 441
Call Teach Mode (*82) 442
Listen In (*83) 442
Miscellaneous 443
Show Account Balance (*61) 443
Wakeup Call (*62) 443
Request Call Details (*63) 444
Clean up an Extension (*84) 444
Add to White List (*91) 444
Add to Black List (*92) 445
Call Record (*93/*94) 445

25 Voicemail **447**
Setting up the Voicemail Account 448
Changing the PIN 448
Record Your Name 448
Record a Personal Welcome Message 449
Accessing the Voicemail System 449
Forwarding a Message 450
Leaving Voicemail Messages 451
Composing a New Message 451
Personal Greetings 452
Recording/Activating Personal Greetings 452
Hearing Your Personal Greetings 453
Advanced Features 453
Send a Voicemail Message Without Ringing Extension(s) 453
Transfer a Call Directly to Someone's Voicemail 454
Listen to Voicemail on Cell Phone 454
Voicemail Notification 454
Via Email 454
Via Cell Phone 455
Voicemail Feature Codes 455
Send Voicemail to Email Account (*95/*96) 455
Go to Voicemail (*97) 456
Go to Group Mail (*97) 456
Clear Message Waiting Indicator (*99) 458

26 Cell Phones **459**
Cost Savings 461
Callback 461
Calling Card Account 462
Configuring the Cell Phone 463
Add a Cell Phone to Your Account 463
Safeguard Against Loss-of-Signal Events 466
Ring My Cell Phone When Voicemail Arrives 466
Feature Codes 468
Retrieve Call From Cell Phone (*51) 468
Move Current Call to Cell Phone (*52) 468
Call Cell Phone of the Extension (*00) 469
Personal Virtual Assistant 470

Appendix A. Working with CSV Files **475**

Appendix B. SIP Overview **499**

Appendix C. snom ONE and Exchange **527**

Glossary **535**

Index **555**

snom ONE

Part I
Getting Started

Chapter 1

GETTING STARTED

Welcome to snom ONE, your state-of-the-art IP telephone system. Administrating a VoIP system can be a daunting task for administrators unfamiliar with VoIP. This guide is designed to help you plan and configure snom ONE Voice over IP (VoIP) deployments ranging in complexity from a small office using the Internet for SIP trunks to a large, multi-national conglomerate of snom ONE systems.

snom ONE is the answer to all your IP telephone system needs.

About snom ONE

snom ONE is a SIP-based IP telephone system which is implemented in a back-to-back user agent (or B2BUA), so all traffic between two endpoints traverses the system (Figure 1-1). This gives the system complete control of the call state and allows it to participate in all call requests. It also allows it to perform a number of functions that are impossible using the SIP proxy model. A few such functions are forking calls to the cell phone, returning them to the system, if needed, and connecting phones remotely to the system. The B2BUA also facilitates advanced media features such as call recording, barge, listen in, and whisper, as well as ensuring two-way audio session is established.

Figure 1-1. B2BUA Architecture

The system is easily portable to most operating systems and requires only a small amount of memory. Due to the need for speed, snom technology does not use a traditional database to store its information. Doing database lookups can be slow in a very busy system. Having a data structure in memory with the necessary information to authenticate a phone is much faster.

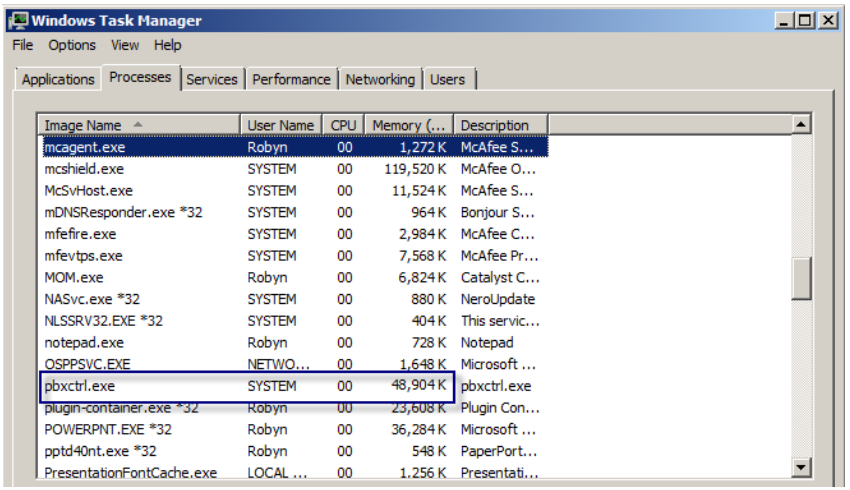
The snom ONE telephone system is a software-based solution and executes several measures to preserve call quality:

- A high-scheduling priority is used with applications that are real-time critical.
- The snom ONE measures CPU usage and rejects calls if the load becomes too high.
- When too many calls are coming in during a short period (call bursts), the system also rejects calls.

While these measures are important, the performance of the software depends largely on the hardware being used.

Memory/Hardware Requirements

The snom ONE system consumes only a small amount of memory. In the image shown below, a snom ONE system uses under 50 MB of RAM, which is not unusual for a lightly loaded system.


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Image Name User Name CPU Memory (... Description
mcagent.exe Robyn 00 1,272 K McAfee S...
mcshield.exe SYSTEM 00 119,520 K McAfee O...
McSvHost.exe SYSTEM 00 11,524 K McAfee S...
mDNSResponder.exe *32 SYSTEM 00 964 K Bonjour S...
mfefire.exe SYSTEM 00 2,984 K McAfee C...
mfevtps.exe SYSTEM 00 7,568 K McAfee Pr...
MOM.exe Robyn 00 6,824 K Catalyst C...
NASvc.exe *32 SYSTEM 00 880 K NeroUpdate
NLSSRV32.EXE *32 SYSTEM 00 404 K This servic...
notepad.exe Robyn 00 728 K Notepad
OSPPSVC.EXE NETWO... 00 1,648 K Microsoft ...
pbxctrl.exe SYSTEM 00 48,904 K pbxctrl.exe
plugin-container.exe *32 Robyn 00 23,608 K Plugin Con...
POWERPNT.EXE *32 Robyn 00 36,284 K Microsoft ...
pptd40nt.exe *32 Robyn 00 548 K PaperPort...
PresentationFontCache.exe LOCAL ... 00 1,256 K Presentati...

For a heavily loaded system, we recommend 2 GB of RAM. However, the system can run on machines with far less RAM, but this will depend on your operating system.

Factors influencing memory requirements include the number of voice mails that accumulate, how much logging information is stored on the system, and the number of CDRs you store. To keep 2 weeks' worth of information on a heavily trafficked system, you will need sufficient memory to store that information. The following table reflects our recommended minimums:

	10 Extensions	20 Extensions	150 Extensions
Memory*	40 MB	50 MB	150 MB
Hard Disk**	100 MB	100 MB	150 MB

* Memory requirements will increase according to voicemails, CDR duration, etc.
** Hardware requirements are significantly impacted by recordings, as they consume large amounts of disk space.

CPU requirements can be a challenge; however, the affinity mask can be used to improve the performance of the PBX. The ideal scenario will be to have a dual-core CPU, wherein the PBX is bound to one of the cores. This setting instructs the operating system to run the PBX on the specified core, eliminating the context switching issues that can cause problems for time-critical RTP threads.

When determining hardware requirements, you need to factor in the number of parallel calls, the number of registrations that will be kept alive on the system, and transcoding issues (i.e., will the CPU need to translate the codecs?). If the CPU only has to pass the packets through, the CPU performance is practically limited by the I/O-subsystem.

Hard disk space is also dependent on whether or not you'll be recording calls and the length of time the recordings will be kept on the system. At minimum, 100 MB is needed, but call volume and other variables will determine whether 100 MB is really sufficient.

Although the hard disk requirement for the installation is minimal (less than 20 MB), keeping an eye on the system once it has been in production for a while is essential. Additional languages, recorded calls, and log files can fill the disk quickly.

USB Device

The snom ONE software has been loaded onto the 1 GB USB drive that was shipped with this book. This section contains information about the USB drive.

Warnings

The USB drive is for indoor use or storage with a temperature range between +0°C and +70°C. Not for outdoor use! Do not use or store the product in rooms with high humidity (for example, in bathrooms, laundry rooms, damp basements). Do not immerse the product in water, and do not spill or pour liquids of any kind onto or into any part of it. Do not use the product in surroundings at risk for explosions, and do not use the handset in such surroundings (paint shops, for example). Your device may contain small parts, so keep them out of the reach of small children.

Standards Conformance

This device is CE and FCC-certified and meets European and U.S. health, safety, and environmental standards. Unauthorized opening, changing, or modifying the device will cause the warranty to lapse and may also result in the lapse of the CE and FCC certifications. In case of malfunction, contact authorized service personnel, your reseller, or snom technology.

Disposal

This device is subject to European Directive 2002/96/EC and may not be disposed of with general household garbage. The separate collection and proper disposal of electrical and electronic devices serves to protect human health and the environment. It also provides a vehicle for using and reusing resources prudently and rationally. If you do not know where you may dispose of the device at the end of its lifespan, contact your municipality, your local waste management provider, or your seller. Disposal of electrical and electronic products in countries outside the European Union should be done in line with local regulations. Please contact local authorities for further information.

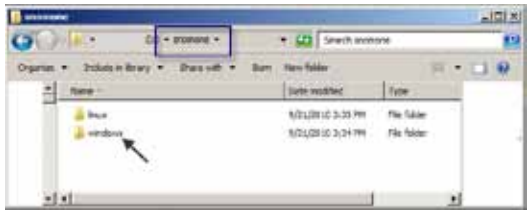
Installing the Software

The snom ONE software has been loaded onto the USB drive that was shipped with your order. Follow the instructions below to complete the installation.

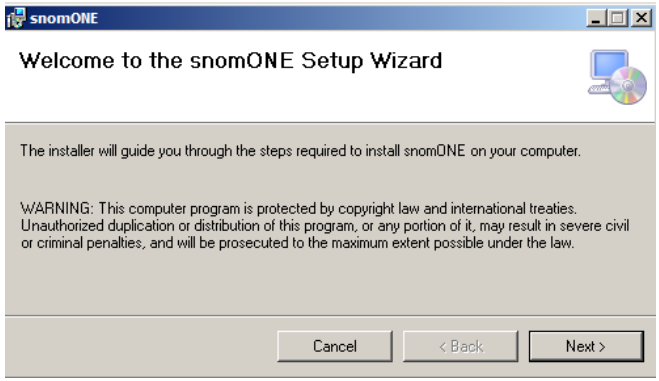
Note: If you purchased this book without the software, you may download snom ONE free at `http://www.snom.com/products/ip-pbx/snom-one`. Click the **snom ONE free** link at the top-right corner, fill out the form, then click **Submit**. Your personal download link will be sent via email (check your spam folder). Double-click the `setup.exe` file inside the email to install the software.

Windows Installations

1. Put the USB drive into your computer. The software will be listed with your standard disk drives.
2. Double-click the `snomone` folder.
3. Double-click the `windows` folder.



4. Double-click `setup.exe`.
5. Click **Next** at the welcome wizard.


snomONE
Welcome to the snomONE Setup Wizard
The installer will guide you through the steps required to install snomONE on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

6. Choose an installation location or accept the default, then click **Next**.

snomONE
Select Installation Folder
The installer will install snomONE to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files (x86)\snom\snomONE\
Browse...
Disk Cost...

Note: If you are installing the software on a 64-bit system, the default directory path will be as follows:

snomONE
Select Installation Folder
The installer will install snomONE to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files\snom\snomONE\
Browse...
Disk Cost...
Install snomONE for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >

7. Click **Next** to start the installation.

snomONE
Confirm Installation
The installer is ready to install snomONE on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >

The installation will take a minute to install.

8. Click **Close** when the installation is complete.

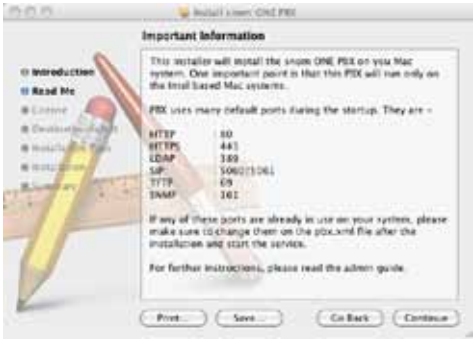
MAC OS Installations

This section explains how to install snom ONE for Mac OS (tested on Darwin). Currently, we support only Intel-based hardware.

1. Navigate to `http://wiki.snomone.com`, and click **Downloads** at the left.

2. Click **Mac - Installer - New Installations Only**.
3. Download the installation package.
4. Unzip the zip file by double-clicking it.
5. Execute the installer contained in the zip file.
6. At the Welcome screen, click **Continue**.

7. At the **Important Information** page, click **Continue**.



8. Take a moment to look through the license agreement, then click **Continue**.

9. To continue the installation, click **Agree**.

To continue installing the software you must agree to the terms of the software license agreement.
Click Agree to continue or click Disagree to cancel the installation and quit the installer.
Read License
Disagree
Agree
Print...
Save...
Go Back
Continue

10. To install snom ONE to the default directory, click **Install**. To install it to a new location, click **Change Install Location** and select a location.

11. At the password screen, enter your password and click **OK**.

12. Click **Close** when the installation is complete.

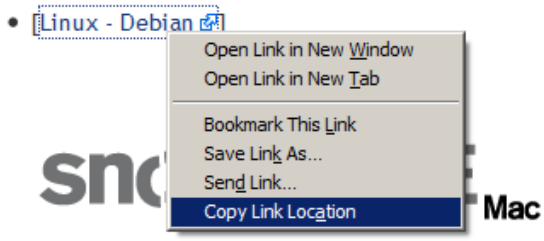
To log into snom ONE, enter `http://localhost` into a web browser. If you are using a different HTTP port, then enter `localhost:<port>` (e.g., `localhost:80`).

Linux Installations

Debian

1. Go to www.wiki.snomone.com, and click **Downloads** at the left.

2. Right-click **Linux - Debian** and copy the link location.



3. Download the file onto your Linux box using the following command:
`wget <linklocation><previously saved>`

   For example:

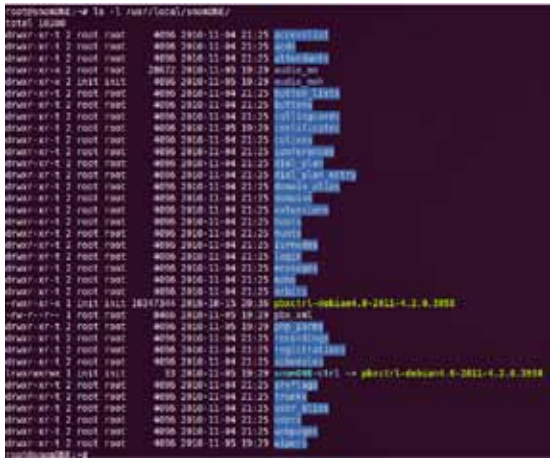
   ```
   wget http://downloads.snom.net/snomONE/debian/
   snomone-debian4-2011-4.2.0.3958.deb
   ```

root@snomONE:~# wget http://downloads.snom.net/snomONE/debian/snomone-debian4-2011-4.2.0.3958.deb
--2010-11-05 19:20:55-- http://downloads.snom.net/snomONE/debian/snomone-debian4-2011-4.2.0.3958.deb
Resolving downloads.snom.net... 188.40.44.83
Connecting to downloads.snom.net|188.40.44.83|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17021552 (16M) [application/x-debian-package]
Saving to: `snomone-debian4-2011-4.2.0.3958.deb'
100%[=>] 17,021,552 824K/s in 21s
2010-11-05 19:21:16 (793 KB/s) - `snomone-debian4-2011-4.2.0.3958.deb' saved [17021552/17021552]
root@snomONE:~#

4. To install the software, execute the following command with root privileges:

   ```
   dpkg -i snomone-debian4-2011-4.2.0.3958.deb
   ```

   The installed files are located in `/usr/local/snomONE` as shown below:



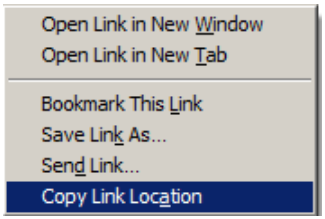
If you need to uninstall snom ONE, execute the following command:

```
apt-get remove snomone
```

Cent OS

1. Go to www.wiki.snomone.com, and click **Downloads** at the left.

2. Right-click **Linux - CentOS** and copy the link location.



3. Download the file onto your Linux box using the following command:
   `wget <linklocation><previously saved>`

   For example::

   ```
   wget http://downloads.snom.net/snomONE/centos32/
   snomone-CentOS5-2011-4.2.0.3958.bin
   ```

```
root@snomONE:/tmp# wget http://downloads.snom.net/snomONE/centos32/snomone-CentOS5-2011-4.2.0.3958.bin
--2010-11-05 19:34:13--  http://downloads.snom.net/snomONE/centos32/snomone-CentOS5-2011-4.2.0.3958.bin
Resolving downloads.snom.net... 188.40.44.83
Connecting to downloads.snom.net|188.40.44.83|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17013688 (16M) [application/octet-stream]
Saving to: `snomone-CentOS5-2011-4.2.0.3958.bin'

100%[======================================================================================>] 17,013,688   825

2010-11-05 19:34:34 (811 KB/s) - `snomone-CentOS5-2011-4.2.0.3958.bin' saved [17013688/17013688]

root@snomONE:/tmp#
```

4. To make the file executable once the download is complete, enter the following command:

   ```
   chmod +x snomone-CentOS5-2011-4.2.0.3958.bin
   ```

5. To execute it, enter the following command:

   ```
   ./snomone-CentOS5-2011-4.2.0.3958.bin install
   ```

   The installed files are located in `/usr/local/snomONE` as shown below:

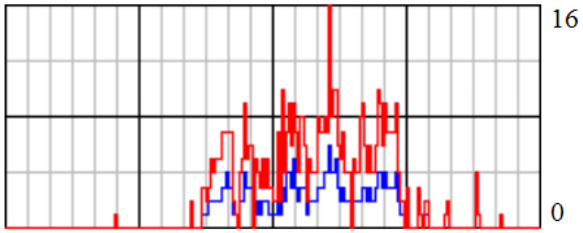
```
root@snomONE:~# ls -l /usr/local/snomONE/
total 10280
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 accesslist
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 acds
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 attendants
drwxr-xr-x 2 root root    28672 2010-11-05 19:29 audio_en
drwxr-xr-x 2 init init     4096 2010-11-05 19:29 audio_moh
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 button_lists
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 buttons
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 callingcards
drwxr-xr-t 2 root root     4096 2010-11-05 19:29 certificates
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 colines
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 conferences
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 dial_plan
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 dial_plan_entry
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 domain_alias
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 domains
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 extensions
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 hoots
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 hunts
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 ivrnodes
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 login
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 messages
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 mohs
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 orbits
-rwxr-xr-x 1 init init 10347344 2010-10-15 20:36 pbxctrl-snomone-CentOS5-2011-4.2.0.3958
-rw-r--r-- 1 root root     8466 2010-11-05 19:29 pbx.xml
drwxr-xr-t 2 root root     4096 2010-11-05 19:29 php_parms
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 recordings
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 registrations
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 schedules
lrwxrwxrwx 1 init init       33 2010-11-05 19:29 snomONE-ctrl -> pbxctrl-snomone-CentOS5-2011-4.2.0.3958
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 sruflags
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 trunks
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 user_alias
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 users
drwxr-xr-t 2 root root     4096 2010-11-04 21:25 webpages
drwxr-xr-t 2 root root     4096 2010-11-05 19:29 wipers
root@snomONE:~#
```

To uninstall the software, execute the following command:

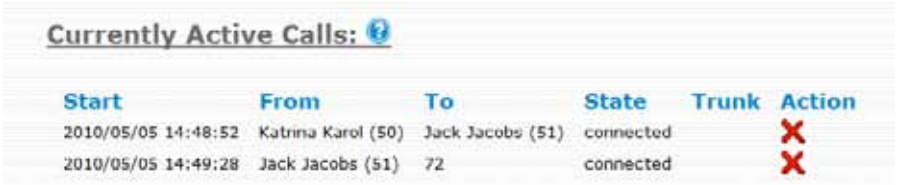
```
./snomone-CentOS5-2011-4.2.0.3958.bin uninstall
```

Upgrading the Software

Software upgrades can be downloaded from wiki.snomone.com. To avoid interrupting calls, perform system upgrades during off hours. If you need to upgrade the system when the system is active, you can send a page announcing the upgrade, or in cases where only a few people are involved, barge into the call and inform the participants of the upgrade. The **Maximum Number of Calls** setting can also be used to restrict call activity (see page 48). Configure this setting to `0` so that no new calls can be established on the system. To check the status of the system, navigate to **Admin** > **Status** > **Graphs**. A busy system will show active calls on the system graphs.



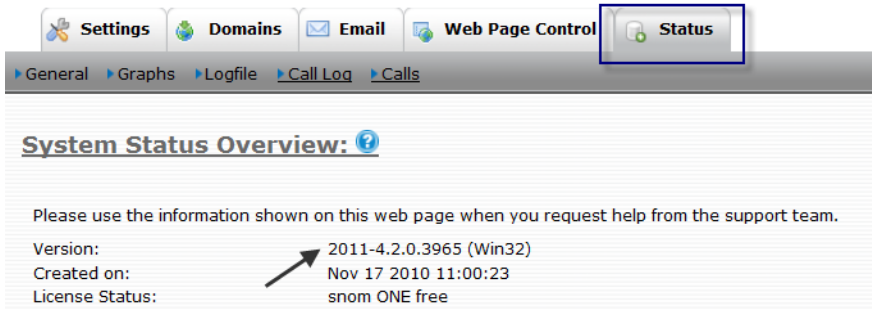
Another way to determine how many active calls are on the system is to check the call list (from the domain settings, click **Status** > **Calls**).



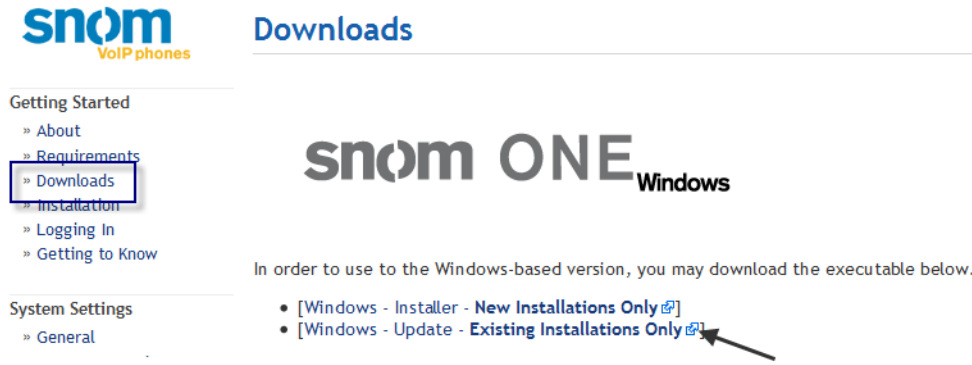
Manual Software Upgrades (Windows)

Manual upgrades can be done by replacing the `pbxctrl.exe` file. Before the upgrade, you might want to make a backup of the working directory in the event you want to revert to the former software version.

1. Determine the version number of the current software by going to **Admin** > **Status**.



2. Navigate to the working directory and rename the `pbxctrl.exe` file so that it corresponds with the old version number (e.g., `pbxctrl-2.0.3.1713`). Keep the file in the directory so that you can later determine which software version is associated with which file. This step can be done while the system is running.
3. Go to wiki.snom.com and download the new executable (click the **Existing Installations Only** link).



4. Place the file into the `snomONE` working directory.
5. Rename the new file `pbxctrl.exe`.
6. Restart the system.

Mac OS Upgrades

Installer Upgrade

To upgrade snom ONE on a MAC, navigate to `wiki.snomone.com`, select **Downloads**, and follow the Mac OS installation instructions on page 7 of this manual. If for any reason you see errors, follow the steps below:

1. Back up the working directory. This is where all the configuration files reside. The default working directory is `/usr/Applications/snomone`.
2. Manually delete `/Library/snomone/*`
3. Install the new version.

In some cases, the software may have installed successfully, but still the old version is running. In such cases, stop the PBX, remove the link, then recreate it. Instructions are detailed below:

1. Stop the PBX using the following command:

   ```
   sudo /Library/StartupItems/PBX/PBX stop
   ```

2. Remove the old link to `pbxctrl-darwin9.0` by entering the following command:

   ```
   rm pbxctrl-darwin9.0-<old file>
   ```

3. Recreate the link using the following command:

   ```
   ln -s <new file> pbxctrl-darwin9.0
   ```

4. Restart the PBX using the following command:

   ```
   sudo /Library/StartupItems/PBX/PBX start
   ```

Manual Upgrade

1. Download the new version from `wiki.snomone.com` by clicking **Downloads** and right-clicking the file.
2. Move the file to the `/Library/snomone` directory.
3. If you need to change the permissions to the file once moved, open a terminal window and execute the following commands:

   ```
   cd /Library/snomone
   ```

```
sudo chown rootadmin <newly installed version>
sudo chmod 775 <newly installed version>
```

4. Once the file is in the correct location and has the appropriate permissions set, follow the instructions below:

```
$ sudo /Library/StartupItems/PBX/PBX stop
$ cd /Library/snomone
$ rm pbxctrl-darwin9.0
$ ln -s <newly installed version> pbxctrl-darwin9.0
$ sudo /Library/StartupItems/PBX/PBX start
```

Linux Upgrades

All configuration will be kept; however, we recommend you do a full backup of your `/usr/local/snomONE` directory before doing the update.

Debian

1. Download the correct installer for your platform.
2. Execute the following command with root privileges:

```
dpkg -i snomone-debian4-2011-4.2.0.3958.deb
```

Cent OS

1. Download the correct installer for your platform.
2. Execute the following commands with root privileges:

```
chmod +x snomone-CentOS5-2011-4.2.0.3958.bin
./snomone-CentOS5-2011-4.2.0.3958.bin update
```

Logging In

Once the software has been installed, the snom ONE will run as a service. To access it, bring up a browser from the machine on which the software has been installed and enter `http://localhost`.

Note: If there is a firewall running on the system, be sure that it allows access to HTTP as well as the other ports of the system (see page 53).

The login screen shown below will be displayed:

Figure 1-2. Login Levels

Login Levels

snom ONE includes three main login levels—administrator, domain administrator, and user— that provide access to different web interfaces. The login levels are shown in Figure 1-2, and the web interfaces for each login type are shown in Figure 1-3:

Figure 1-3. snom ONE Web Interfaces

The **Automatic** login type will default to the highest login level of the person logging in. Administrators and domain administrators who want to log in as a user must enter their extension number and choose **User Login** from the dropdown. Instructions for each login type are detailed below.

Login Types

- For users:
  - Account: Extension number (e.g., `509`)
  - Password: Extension password
  - Login Type: **Automatic**
- For system administrators: If you are logging in as an administrator, use the following account information to log in:
  - Account: `admin`
  - Password: The password field is blank by default.
  - Login Type: **Automatic**.

    Note: When either a system or a domain administrator logs in as a user, **User Login** must be selected from the dropdown.
- For domain administrators: If you are logging in as a domain administrator, use the following account information to log in:
  - Account: Extension number (e.g., `555`)
  - Password: Extension password
  - Login Type: **Automatic**
- To access the WAC:
  - Account: Extension number (e.g., `509`)
  - Password: Extension password
  - Login Type: **Console Login**

Activating Your License

Your snom ONE license will need to be activated before you can register extensions to the system. The activation code is located on the back cover of this book near the **Product key** barcode. To activate your license, complete the following steps:

1. Click **Admin**.

2. Click the **Settings** tab, then click **License** as shown below:

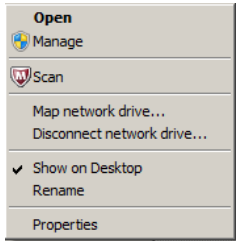
3. Enter your activation code into the **Code** box (the activation code is located on the back cover of this book near the **Product key** barcode).

Restarting the System

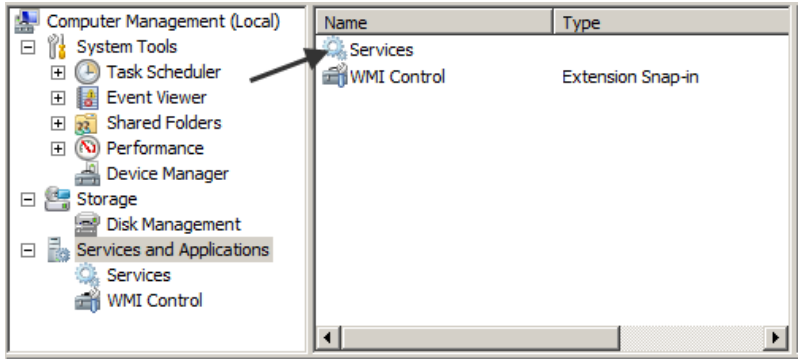
Various system configurations require a system restart. You can do this by either restarting the computer or restarting the system. When restarting the system, use one of the following methods.

Restarting From Windows (Service Control Manager)

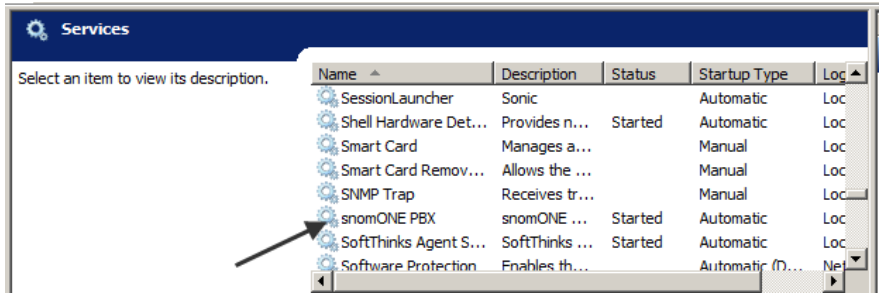
1. Right-click **My Computer**.
2. Click **Manage.**



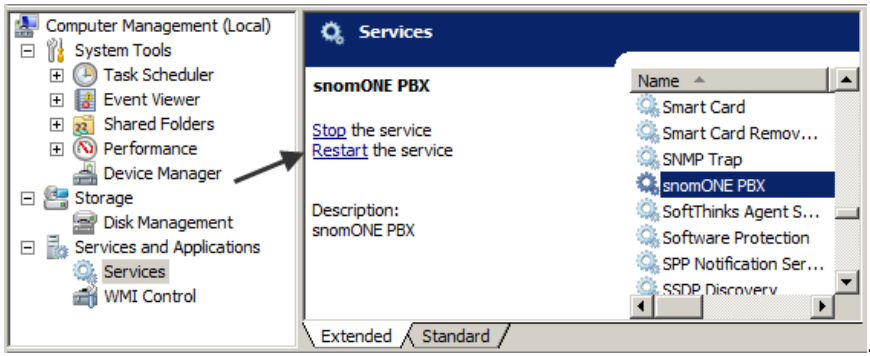
3. Click **Service Applications**, then click **Services**.



4. From the right-hand pane, click `snomONE PBX`.



5. Click **Restart**.



Restarting From a Command Line

The system can be stopped and restarted from the command line:

- `net stop snomone`
- `net start snomone`

Restarting From Mac OS

The simplest way to restart snom ONE from a Mac is to restart the Mac, but this may not be desirable in many cases. In such cases, you can start and stop snom ONE from the command line:

- `/Library/StartupItems/snom/snomone stop`
- `/Library/StartupItems/snom/snomone start`

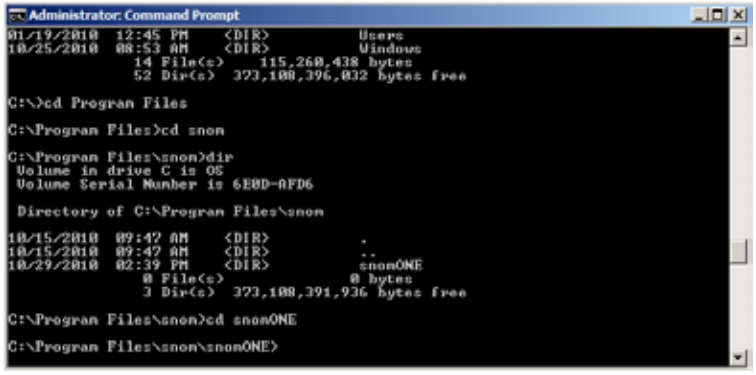
Restarting From a Linux Environment

- `/etc/init.d/snomONE restart`
- `/etc/init.d/snomONE stop`

Manually Starting the Service

To manually start the system with logging:

1. Open a command prompt.
2. Go to the snom ONE working directory.



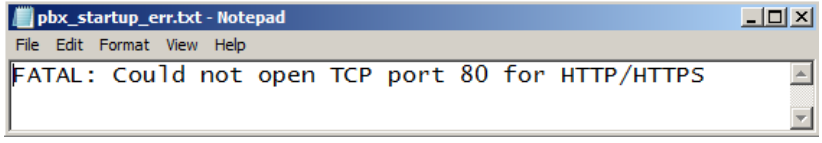
3. On Windows, enter `.\pbxctrl.exe --dir . --no-daemon --log 9`
4. On Linux, enter `./snomONE-ctrl --dir . --no-daemon --log 9`
5. Press **Enter**.

This will force the service to start at log level 9, which will help you diagnose issues that stop the service from fully initializing.

When the System Fails to Restart

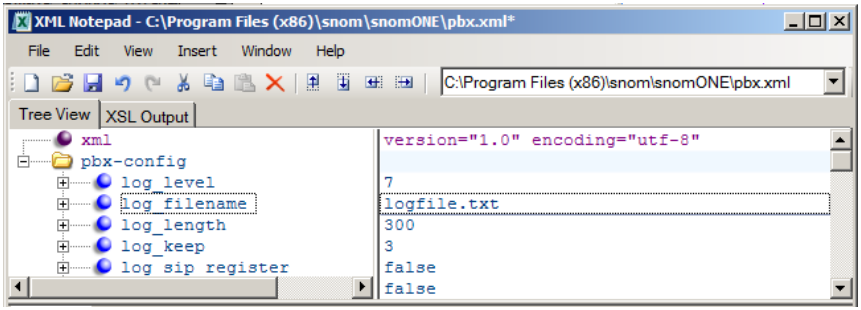
When the system fails to start, the system attempts to write the error message to the log file in accordance with the *`log_filename`* parameter contained in the `pbx.xml` file; however, if the `pbx.xml` file has not been set up properly or if the system crashed before the error message was written, the administrator will be unable to determine the cause of the error.

A way around this issue is to rely on the `pbx_startup_err.txt` file. This file is located in the `snom/snomONE` folder and indicates why the system either crashed or did not come up the last time an attempt was made. Following is a sample error message:

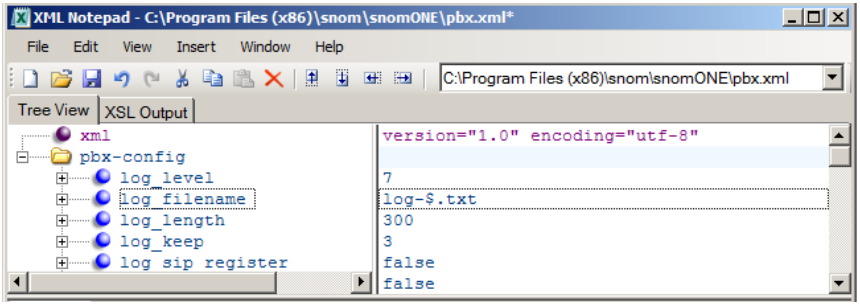


Setting up the Log File

If you want to log the PBX messages (error or not), the *log_filename* parameter in the pbx.xml file may need to be modified so that the value of the *log_filename* parameter includes a dollar sign ($); otherwise, your system's performance will become unstable. The following sample shows a problematic value in the *log_filename* field.



To change the value, open the pbx.xml file using an XML editor. Click in the text and replace it with log-$.txt.



Technical Support

Technical support for snom ONE is available through the wiki, the online help system, and the forum. If you cannot find an answer to your question through these sources, you can also open a ticket with snom ONE support. Each support option is detailed below.

Wiki

The view the knowledge data for snom ONE, go to wiki.snomone.com.

Online Help

To access online help, click the **Help** link at the top of each page.

Forums

To join the forum, go to forum.snom.com.

Submit a Ticket

To submit a ticket or view existing tickets, go to support.snom.com, and log in or register a new account:

Documentation

The following typographic and usage conventions occur in this book:

Typeface	Description	Example
Bold	Names of tabs, settings, and buttons	Navigate to **Admin** > **Settings** > **Logging.**
`monospace`	File and directory names, examples of program code, command strings, and user input.	▪ The default recording name is `$r/$d/$t-$i-$u-$n.wav` ▪ Place the file into the `recordings` directory. ▪ A typical dial plan would include the string `([0-9]*)@.*` as pattern and `sip:\1@\r;user=phone` as the replacement.
`monospace italic`	Names of parameters	▪ Modify the *`cdr_field_separator`* parameter.

Feedback and comments can be sent to feedback@snom.com.

snom ONE

Part II
Administering the System

Chapter 2

SYSTEM SETTINGS

The snom ONE telephone system encompasses three different access levels—administrator, domain administrator, and user—each providing a different web interface (depicted earlier on page 18). The system administrator has control of the entire system, while the domain administrator has control of only the domain. This setup enables the administrator to assign responsibilities related to user accounts and other non-system-related settings to another individual without compromising system configurations. This chapter discusses administrator-level settings only. Configurations that can be made by the domain administrator are discussed in Chapter 3.

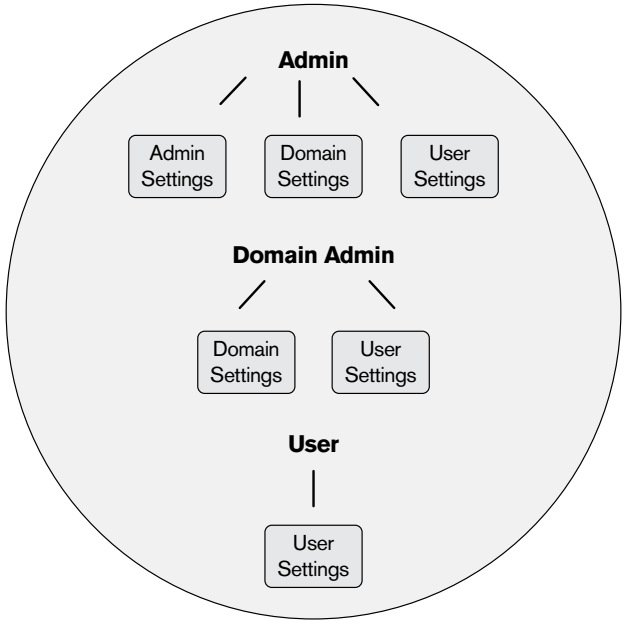


Figure 2-1. snom ONE Web Interfaces (Admin, Domain Admin, and User)

To access the administrator settings:

1. Log in as admin. The following screen will be displayed.

snom ONE
Home
Help
Logout
Settings
Accounts
Trunks
Dial-Plans
Status
Admin
Domain Administration Preconfigured Domain (pbx.company.com)
Domain Settings are necessary to customize the behavior of the PBX in this domain. Here you can define how features are mapped to star codes.
* * *
Accounts are anything that you can dial on your PBX. Accounts include Extensions, Auto Attendants, Conference Rooms. These numbers may be service numbers of the PBX as well as the numbers of your extensions.

2. Click **Admin**. The new screen includes the four tabs shown below. These tabs can be seen only by administrators.

snom ONE
Home
Help
Logout
Settings
Domains
Email
Web Page Control
Status
General
Graphs
Logfile
Call Log
Calls
System Status Overview:
Please use the information shown on this web page when you request help from the support team.
Version: 2011-4.2.0.3965 (Win32)
Created on: Nov 17 2010 11:00:23
License Status: snom ONE free
License Duration: Permanent
Additional license information: Extensions: 10/10 Accounts: 27/30 Upgrade: 01 01 2013
Working Directory: C:\Program Files\snom\snomONE
MAC Addresses: 204133594EFF 6CE120524153 A4BADB02092D
Calls: 0/0 (CDR: 4/47/4) 0/0 Calls
SIP packet statistics: Tx: 278 Rx: 25
Emails: Successful sent: 0 Unsuccessful attempts: 0
Uptime: 2010/11/17 13:41:47 (uptime: 0 days 00:34:36) (7MB/4087MB 56% 18156352-0) WAV cache: 0
Number of HTTP sessions: Sessions: PAC=0, HTTP=1; Threads: SIP=0, HTTP=1

The settings associated with the administrator tabs are briefly outlined in Figure 2-2 and are described in more detail in Table 2-1.

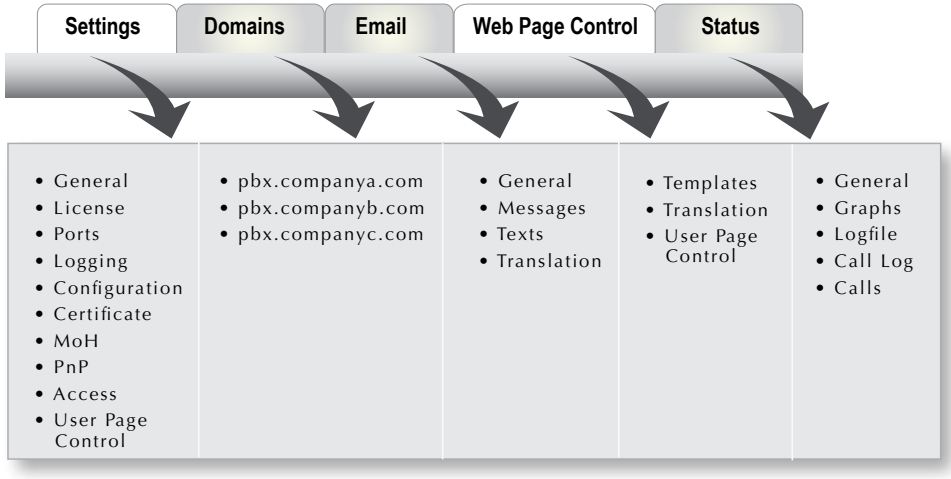


Figure 2-2. Outline of Adminstrator Web Interface

The following table provides an overview of the various topics that are available from the administrator's view of the web interface. These topics are discussed in more detail throughout this chapter.

Table 2-1. Menu Tree of Administrator Tabs

Tab/Link Name	Description
Settings	
General	This page allows you to configure global system settings (IVR, tone, and web languages), including performance, password, and SIP settings.
License	This is where you activate your license code.
Ports	The ports that are used for the system are specified here.
Logging	The settings on this page are designed to help you debug issues.

Tab/Link Name	Description
Configuration	From this page, you can restore the system's configuration, including recordings and customized files in the `tftp` server directory. You can also request configuration information from a service provider, reload configuration files if you want to change them without restarting the system, or schedule a system reboot.
Certificate	From this page, you can install a certificate and private key to ensure secure communication. The certificate will be checked by clients that need to trust you. The private key will be used for encrypting messages.
MoH	The settings on this page allow you to specify which music on hold sources will be available on the system.
PnP	From this page, you can provide parameters to change the generation of plug and play files.
Access	You can control which IP addresses may access the snom ONE service here.
Domains	From the **Domains** tab, the administrator can view and edit the domain.
Email	
General	This page allows you to configure the mail client settings that will be used by the system when sending out emails.
Messages	The settings on this page allow you to specify which events warrant an email notification and who should receive that notification. Examples include call rejection due to CPU load and call disconnection because of one-way audio.
Web Page Control	
Templates	This page allows you to change the look and feel of the PBX web pages. It also allows you to change the various email templates, phone configuration templates, style sheets, etc.
Translation	This page allows you to change the translation of text that is used in various places throughout the web interface.

Tab/Link Name	Description
User Page Control	This page lets you control which settings will be displayed on the user's web interface.
Status	
General	This page shows you the status of your system (e.g., the release of software you are running, the type of software, the expiration date, etc.).
Graphs	This page displays a graphical representation of CPU usage, current calls and registrations, and the MOS for extension and trunk calls.
Logfile	This page displays SIP messages, which can be used for trouble-shooting.
Call Log	A list of calls that have been made through the system is displayed.
Calls	A list of active calls is displayed.

Directory Structure

Directory Tree

While most of the system settings can be configured from the web interface, the administrator will need to access the file system at times. This section provides a brief overview of the files that are part of the system and explains why you may need to access them.

All files related to the system are located in `C:\Program Files\snom\snomONE`, which is the system's default working directory. The main program that runs the software is `pbxctrl.exe`, and the global configuration file is `pbx.xml` (Figure 2-3). The folders within the `snomONE` directory contain files that hold information about accounts, trunks, audio prompts, features, and many other parts of the system. The majority of folders are composed during installation. However, a few folders (e.g., `cdre`, `cdri`, `cdrt`) are composed only after the phone communicates with the system (i.e., once a call is made or a star code is used).

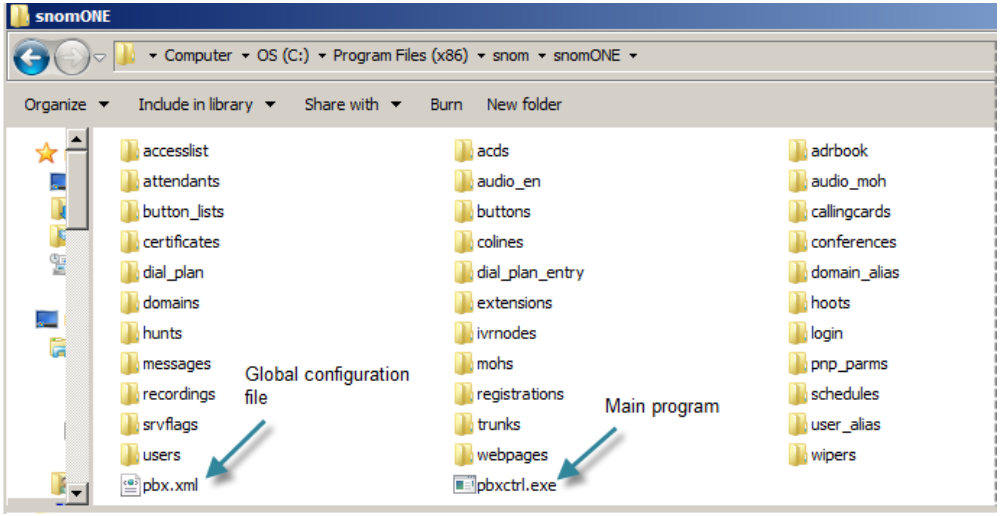


Figure 2-3. snom ONE Directory Structure

Global Configuration File

Some settings cannot be changed via the web interface. Such settings must be modified via the global configuration file (Figure 2-3), a standard XML file that is encoded in UTF-8. Unlike the majority of files that can be modified through the web interface, the global configuration file contains many hidden settings which cannot be changed this way. Changes to this file must be made through either the XML file or by handcrafting a URL that contains the change. With either method, the three important components are the address of the snom ONE system, the name of the setting, and the value. In the sample URL shown below, the address is `pbx`, the setting is `setting`, and the value is being changed to `123`.

Important: Always make a backup before modifying the file!

```
http://pbx/reg_status.htm?save=save&setting=123
```

Once the URL is set, press **Enter**. This is equivalent to pressing the **Save** button when in admin mode in the web interface.

A typical use case for modifying the global configuration file would be to change the format of CDRs (applicable only for CDRs that are exported via simple TCP). To change the CDR format of a system running on a localhost, you would use something similar to

```
http://localhost/reg_status.htm?save=save&cdr_format=$w$5d$25
m$2o$20F$20T$20R$20r$15c$20f$15v
```

where *cdr_format* is the parameter.

Caution: The above link will change your CDR format if you execute it while the system is running on the localhost!

Note: If you want a specific delimiter between the fields, use a comma (e.g., `$w,$5d,$25m,$2o,$20F,$20T,$20R,$20r,$15c,$20f,$15v`). Be careful when choosing a delimiter. If the names or URIs contain those characters, there will be a conflict.

Folder Overview

Table 2-2 lists the folders that are located in `snom/snomONE`:

Table 2-2. Folder Details

Folder Name	Contents
accesslist	IP addresses that have been blocked from accessing the system
acds	Account information about each agent group
adrbook	Contacts that have been added to the domain address book
attendants	Account information about each auto attendant
audio_en	Audio prompts for auto attendant, IVR, etc., and ring tones
audio_moh	Music on hold and universal tones like ringback
button_lists	Button profiles that are on the domain
buttons	Individual buttons that are part of the button profiles
callingcards	Account information about each calling card
cdr	CSV CDRs, if any exist
cdre*	CDRs that contain information about the extension
cdri*	CDRs that indicate the role played by the IVR
cdrt*	CDRs that contain information about the trunk

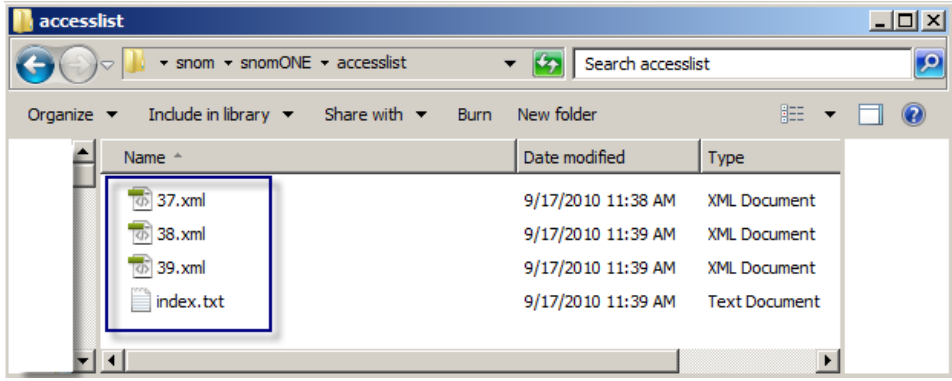
Folder Name	Contents
certificates	Certificates being used by the system.
colines	Central office lines on the trunk
conferences	Account information about conference accounts
dial_plan	Dial plans that are on the domain
dial_plan_entry	Individual pattern and replacement values for each dial plan
domain_alias	Information about the domain when it is associated with an alias
domains	Information about the current state of the domain
email_templates	Custom email templates
extensions	Information about each extension (name, number, MAC, etc.)
generated**	Files that are generated from templates that exist within the system binary
hoots	Multicast paging information
html	Customized HTML files
hunts	Account information about hunt group accounts
ivrnodes	Information about each IVR node account
messages	Voicemail messages
mohs	Available music on hold sources
pnp_parms	Configuration files that are involved in plug and play
recordings	Recorded calls and greetings
registrations	Static registrations
schedules	User-created conferences
srvflags	Account information about service flag accounts
tftp	Firmware and/or provisioning files for the phones
trunks	Information about each trunk on the system
user_alias	Information about each account associated with an alias
users	Information about each account (extension, auto attendant, etc.)
wipers	Conference recordings

* The `cdre`, `cdri`, and `cdrt` folders are generated after the phone contacts the system.

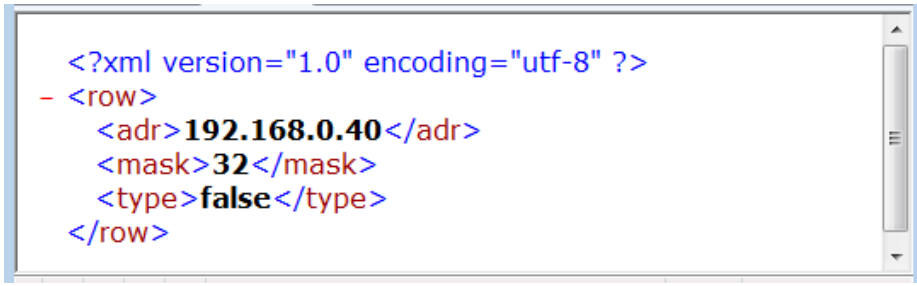
** The `generated` folder is created when the phone contacts the system for its configuration files during plug and play.

Folder Details

Each folder in the snomONE directory contains a list of XML files similar to the following:



Each XML document reflects various XML constructs and concepts:



Each folder in the snomONE directory is detailed below.

- accesslist—The accesslist folder contains IP addresses that have been blocked from accessing the snom ONE service. IP addresses can be blocked/unblocked by the administrator in **Admin** > **Settings** > **Access List**.
- acds—The acds folder contains an XML file for each agent group. Each file includes the possible parameters for the account and any values assigned to those parameters.
- adrbook—The adrbook folder contains contacts that have been added to the domain address book. Each contact has a corresponding XML file.

- `attendants`—The `attendants` folder contains an XML file for each auto attendant. Each file includes the possible parameters for the account and any values assigned to those parameters.
- `audio_*`—The `audio_*` directory contains audio prompts that are used by the auto attendant and IVR node. These prompts affect the language settings that are available from the web interface (see page 43). The files within the directory contain many types of prompts. Following is a summation of the main prefixes.

Prefix	Description
`aa-`	Auto attendant
`bi-`	Built-in numbers
`co-`	Conference
`code-`	Feature-code related
`ex-`	Extension-related
`mb-`	Mailbox
`pb-`	ACD-related
`wk-`	Time-related

Note 1: The directory suffix corresponds with the language of the prompts themselves (i.e., English prompts are contained in `audio_en`). See page 321 for instructions on installing audio prompts for additional languages.

Note 2: The `ringback.wav` and `busy.wav` files are also included in this directory. These files influence the ringback and busy tones that a caller hears during voicemail prompts and IVR interaction (see page 43 for more on tone language).

- `audio_moh`—The `audio_moh` folder contains DTMF tones and music on hold sources.
- `button_lists`—The `button_lists` folder contains the button profiles that are available on the domain.
- `buttons`—The `buttons` folder contains the types of buttons (e.g., private, speed dial, DND) that have been set in the button profiles.

- `callingcards`—The `callingcard` folder contains an XML file for each calling card account. Each file includes the possible parameters for the account and any values assigned to those parameters.
- `cdr`—The `cdr` folder contains the CSV CDRs, if there are any.
- `cdre`—The `cdre` folder contains CDRs that hold extension-related information. A CDR is generated for each call.

```
<?xml version="1.0" encoding="utf-8" ?>
- <row>
    <cmc>50051</cmc>
    <d>1</d>
    <e>1272544320.811</e>
    <f>"Jack Black" <sip:51@pbx.company.com></f>
    <i>3c2d812faa37-rw96l5j1zakt#7101db16da</i>
    <m>true</m>
    <o>0</o>
    <r>"Katrina Kent" <sip:50@pbx.company.com></r>
    <s>1272544316.585</s>
    <t>"Katrina Kent" <sip:50@pbx.company.com></t>
    <u>1</u>
    <vq>VQSessionReport: CallTerm LocalMetrics: CallID:605563f3@pbx
      FromID:"Katrina Kent"
      <sip:50@pbx.company.com>;tag=gyvvqn1m27 ToID:"Jack Black"
      <sip:51@pbx.company.com>;tag=42953 LocalAddr:IP=0.0.0.0
      PORT=53434 SSRC=0xc4a02346 RemoteAddr:IP=0.0.0.0 PORT=0
      SSRC=0x x-UserAgent:pbxnsip-PBX/4.0.1.3475 x-
      SIPmetrics:SVA=RG SRD=62 x-SIPterm:SDC=OK SDR=OR</vq>
  </row>
```

- `cdri`—The `cdri` folder contains CDRs that hold IVR-related information. A CDR is generated for each call.

```
<?xml version="1.0" encoding="utf-8" ?>
- <row>
    <d>1</d>
    <di>5803</di>
    <f><sip:+19781231234@192.168.1.122;user=phone></f>
    <l>en</l>
    <s>1269625831.644</s>
    <t><sip:514@192.168.1.122;user=phone></t>
    <u>72</u>
    <y>attendant</y>
  </row>
```

- `cdrt`—The `cdrt` folder contains CDRs that hold trunk-related information. A CDR is generated for each call.

```
<?xml version="1.0" encoding="utf-8" ?>
- <row>
    <c>1269625825.866</c>
    <d>1</d>
    <e>1269625831.502</e>
    <f><sip:+19781231234@192.168.1.122;user=phone></f>
    <i>8</i>
    <o>I</o>
    <p>udp:192.168.1.91:5060</p>
    <r>+19781231234</r>
    <s>1269625825.695</s>
    <t><sip:514@192.168.1.122;user=phone></t>
    <vq>VQSessionReport: CallTerm LocalMetrics: Timestamps:START=2010-03-26T17:50:26Z
      STOP=2010-03-26T17:50:31Z CallID:b5606103@pbx
      FromID:<sip:9781231234@192.168.1.122;user=phone>;tag=2001826161
      ToID:<sip:514@192.168.1.122;user=phone>;tag=71f3b8135c SessionDesc:PT=0 PD=pcmu
      SR=8000 FD=20 FO=160 FPP=1 PPS=50 PLC=3 LocalAddr:IP=192.168.1.122 PORT=53226
      SSRC=0x10ea8d1d RemoteAddr:IP=192.168.1.91 PORT=49370 SSRC=0x3e069a7d x-
      UserAgent:pbxnsip-PBX/4.0.1.3445 x-SIPterm:SDC=OK SDR=AN PacketLoss:NLR=0.0
      JDR=0.0 BurstGapLoss:BLD=0.0 BD=0 GLD=0.0 GD=0 GMIN=16 Delay:RTD=0 ESD=0
      QualityEst:MOSLQ=4.1 MOSCQ=4.0</vq>
  </row>
```

- `colines`—The `colines` folder contains information about co-lines that are created on the system.
- `conferences`—The `conferences` folder contains an XML file for each conference account. Each file includes the possible parameters for the account and any values assigned to those parameters.
- `dial_plan`—The `dial_plan` folder contains an XML file for each dial plan on the system.
- `dial_plan_entry`—The `dial_plan_entry` folder contains the pattern and replacement values for each entry in the dial plan.
- `domain_alias`—The `domain_alias` folder contains the alias name of each domain. Each alias has an XML file.
- `domains`—The `domains` folder contains details about the domain, such as star codes, password, and PIN requirements.
- `email_templates`—The `email_templates` folder contains customized email templates.

- `extensions`—The `extensions` folder contains an XML file for each extension. Each file includes the possible parameters for the extension and any values assigned to those parameters.
- `hoots`—The `hoots` folder contains an XML file for each paging account. Each file includes the possible parameters for the paging account and any values assigned to those parameters.
- `html`—The `html` folder is used for customizing configuration files, such as `ringtones.xml` and `pnp.xml`. You can download these files from wiki.snomone.com and then place them into the `html` folder. Once the snom ONE is restarted, the new configurations will take effect.
- `hunts`—The `hunts` folder contains an XML file for each hunt group. Each file includes the possible parameters for the account and any values assigned to those parameters.
- `ivrnodes`—The `ivrnodes` folder contains the details of all IVR node accounts. Each file includes the possible parameters for the account and any values assigned to those parameters.
- `messages`—The `messages` folder contains voicemail messages.
- `mohs`—The `mohs` folder contains a WAV file for the sources of music on hold that are available on the system.
- `pnp_parms`—The `pnp_parms` folder contains all configuration files that are involved in plug and play.
- `recordings`—The `recordings` folder contains a WAV file for all greetings and recordings, whether created for personal or system use (e.g., auto attendants, agent groups, and hunt groups). See Chapter 18 for more information on recordings.
- `registrations`—The `registrations` folder is needed for the index file.
- `schedules`—The `schedules` folder contains conferences that were created by users.
- `srvflags`—The `srvflags` folder contains an XML file for each service flag account. Each file includes the possible parameters for the account and any values assigned to those parameters.

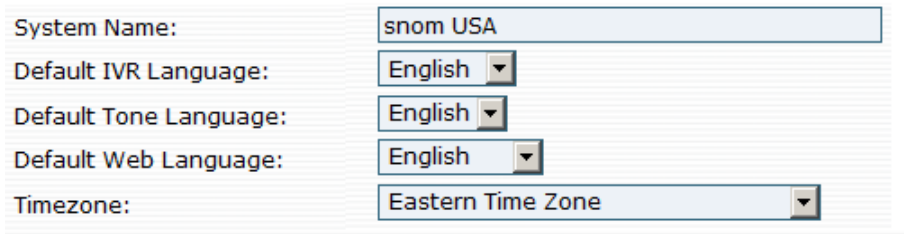
- `tftp`—The `tftp` folder can be used for customizing plug and play. For example, placing the `snom_320_custom.xml` file into the `tftp` folder will provide new settings for the phone.
- `trunks`—The `trunks` folder contains an XML files for each trunk. Each file includes the possible parameters for the trunk and any values assigned to those parameters.
- `user_alias`—The `user_alias` folder contains an XML file for every alias name that is associated with an account (a DID number is considered an alias).
- `users`—The `users` folder contains an XML file for every account on the system (DIDs are not considered a separate account).
- `wipers`—The `wipers` folder contains conference recordings.

Configuring System Settings

This section describes the general administrator settings that are located in **Admin** > **Settings** on the web interface. (You must be logged in as administrator.)

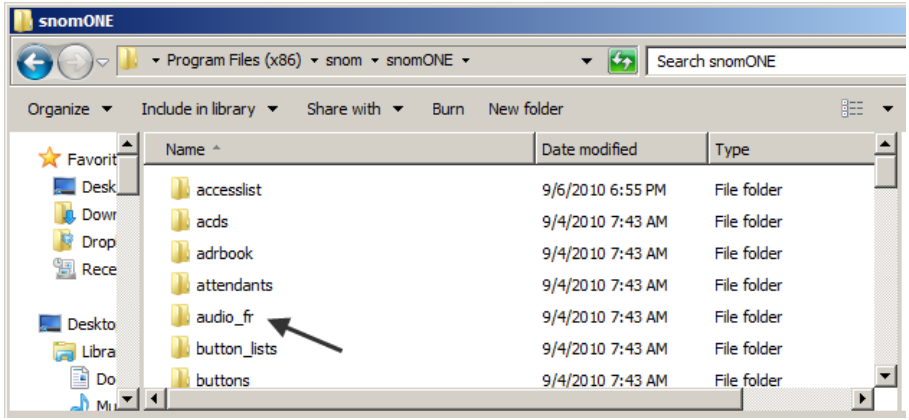
General

- **System Name:** This field allows the administrator to set a name for the system. The name is used in several places to identify the system. For example, when the system sends out emails with system performance information, the system name will be placed into the subject line of the e-mail.



The next four settings pertain to language and time zone. The settings made here by the administrator can be overridden by the domain administrator.

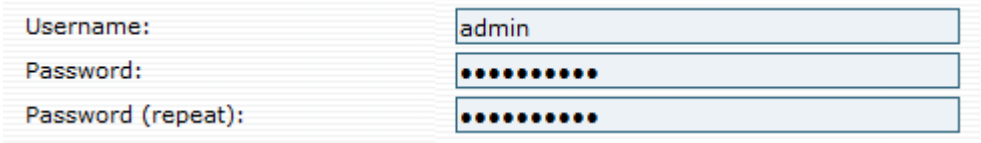
- **Default IVR Language:** This setting represents the language that is used for voicemail and IVR prompts. Only U.S.-English prompts are included in the installer, but additional languages can be installed. See "Audio Prompts" in Chapter 18 for more information on audio prompts and downloading languages.
- **Default Tone Language:** This setting allows you to control the ringback and busy tones that a caller hears during voicemail prompts and IVR interaction. The files that influence this setting are `ringback.wav` and `busy.wav`. These files are located in the `audio_*` directory. The `*` represents a language identifier code (see Table 18-5 for a list of the languages that are supported and their corresponding language identifier codes).



- **Default Web Language:** This setting controls the language used on the web interface. The file that influences this setting is `lang.*.xml`, where `*` represents a language identifier code (see Table 18-5 for a list of the languages that are supported and their corresponding language identifier codes).
- **Time Zone:** The Time Zone setting is used to set the local time zone. It influences the time that appears on a user's mailbox messages, telephone display, and voicemail. The system is capable of dealing with several time zones at once, making it possible for every user to select his or her own time zone.

Administrator Login

The system administrator's login must be protected at all times, so it is imperative that a high-security password be used (see the **Password Strength** setting on page 45). The password is stored in a hashed format and cannot be read from the global configuration file.

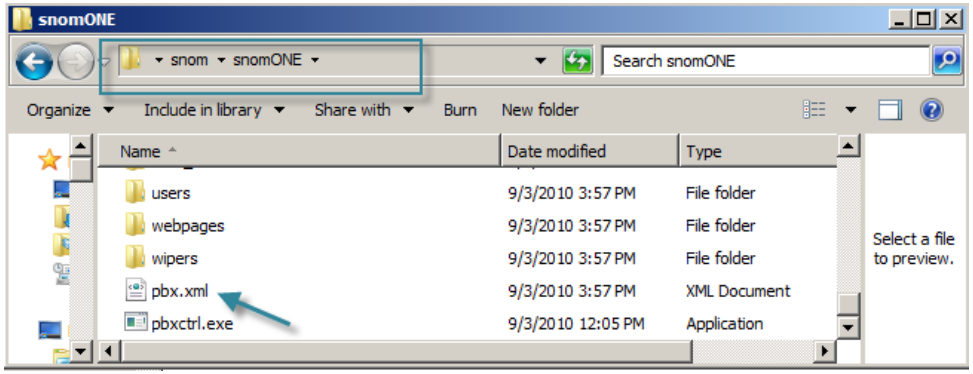


- **Username:** This field sets the administrator's user name. By default, the user name is `admin`, but it can be changed and we recommend doing so.
- **Password:** This field sets the password for the user name from the previous setting. By default, no password has been set, so be sure to set one. This password can be reset in the event it gets lost (see instructions below).

Resetting the Admin Password if Lost

To reset a lost password, you will need to remove the existing password from the global configuration file (from the *`pw_pass`* parameter) and then enter a new one through the web interface. This can be done in Notepad. Instructions are provided below:

1. From a text editor, open the root file (`pbx.xml`). The file path is shown below:



2. Search for the <pw_pass> element tag.

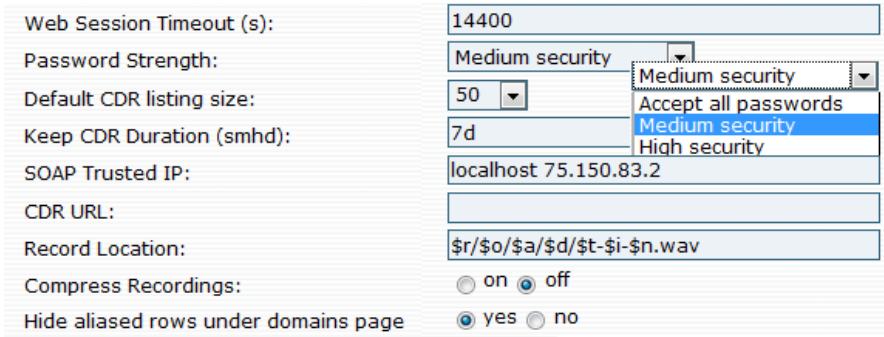
nvite><ip_http_port>80</ip_http_port><ip_https_port>443</ip_https_port><ip_sip_udp_
60</ip_sip_udp_port><ip_sip_tcp_port>5060</ip_sip_tcp_port><ip_sip_tls_port>5061</i
ls_port><ip_snmp_port>161</ip_snmp_port><ip_snmp_community>public</ip_snmp_communit
ftp_port>69</ip_tftp_port><ip_replacement_list/><ip_routing_list/><c2d_root/><max_u
te>10</max_udp_invite><tftp_write>false</tftp_write><tftp_log>true</tftp_log><pnp_u
true</pnp_use_mac><port_begin>49152</port_begin><port_end>64512</port_end><port_bin
rt_bind6/><ip_manual_ip1/><ip_manual_ip2/><http_cert_file/><http_tls_web/><http_rat
tp_rate><pw_user>admin</pw_user><pw_pass>f534983b255eb2820bf3ba1438ddcf65</pw_pass>
sted>127.0.0.1 [::1]

3. Delete the password. (If no text appears between the element tags, then the password field is empty.)

e><tftp_write>false</tftp_write><tftp_log>true</tftp_log><pnp_u
ort_begin>49152</port_begin><port_end>64512</port_end><port_bin
_ip1/><ip_manual_ip2/><http_cert_file/><http_tls_web/><http_rat
in</pw_user><pw_pass></pw_pass><pw_trusted>127.0.0.1 [::1]

4. Save the file.
5. Restart the system.
6. Set a new password through the web interface (**Admin** > **Settings** > **General**).

Appearance



- **Web Session Timeout (s):** This field determines the length of time a web session will stay active before it times out. The duration is set in seconds, and the default value is 3600 (1 hour). Increase or decrease this setting depending on whether you want the system to log you off after a certain period of time. Once timed out, the main login screen will be displayed.
- **Password Strength:** This field is used to specify the types of passwords that are acceptable. The default is "Accept All Passwords," but it is advisable to require medium or high-security passwords. Users should be encouraged to

avoid passwords that are dictionary words and to instead create passwords that are more challenging. A combination of letters, digits, and symbols is recommended.

- **Accept all Passwords:** All passwords will be accepted.
- **Medium Security:** The score must be 120 or higher (see Table 2-3).
- **High Security:** The score must be 200 or higher (see Table 2-3).

Table 2-3. Password Scoring Method

Character Type	Points
Digits	10
Upper/lowercase letters	26
Symbol	28

- **Default CDR listing size:** A Call Detail Record (CDR) is a record that is produced by the system and contains the details of calls that have terminated on the system. CDRs include the date and time the call started, the number that made the call, the number that received the call, and the call duration. Use this field to limit the number of CDRs that will be displayed in the web interface (CDRs can be memory consuming). The default is 30 CDRs. For more information on CDRs, see Chapter 22.
- **Keep CDR Duration:** This setting defines the length of time CDRs are kept on the file system. CDRs can consume large amounts of disk space, so be careful when setting this field. If too many CDRs are on a busy system, the system will not start. The default is 7 days. The duration can be expressed in various time units:
  - Seconds: Enter an `s` after the number (e.g., `60s` for 60 seconds)
  - Minutes: Enter an `m` after the number (e.g., `60m` for 60 minutes)
  - Hours: Enter an `h` after the number (e.g., `24h` for 24 hours)
  - Days: Enter a `d` after the number (e.g., `7d` for 7 days)
- **SOAP Trusted IP:** SOAP (Simple Object Access Protocol) is an XML message-based protocol specification that is used to allow computers to talk

to each other over a network such as the Internet, typically as part of a Web service. SOAP can be used to pass almost any type of data between two applications. Because it is based on XML, SOAP is language- and platform-independent. The two applications could be written in different languages and could run on different operating systems. SOAP is often used to make Remote Procedure Calls (RPCs). When used to encode RPCs, SOAP is used as the request/response protocol. See Chapter 14 for a sample SOAP message.

The **SOAP Trusted IP** field controls a SOAP request coming from random addresses and is available only if the license key contains a SOAP flag. Use this field to specify the IP address or the host names that are permitted to make SOAP requests to the system (i.e., management system). If you want to allow multiple systems to send SOAP requests, use a space to separate the entries.

- **CDR URL:** The CDR URL field controls where the CDRs are written. The system can write CDRs to a SOAP destination and to a CSV file. (The default separator for the values is a comma; however, it can be changed by modifying the *cdr_field_separator* parameter.) To populate the CDR URL field, use the syntax shown in Table 2-4. CDRs can be viewed only after they have been collected and organized through an external call accounting application.

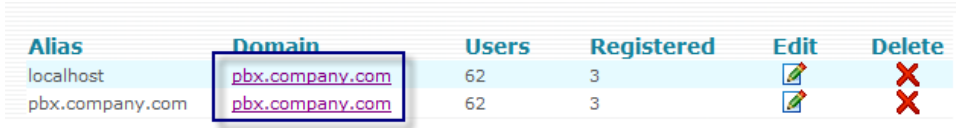
Table 2-4. Syntax Used in CDR URLs

Format	CDR URL Syntax	Description of Syntax
ASCII	`cdr:192.168.1.2:10000`	■ 192.168.1.2 is the IP address ■ 10000 is the TCP port of the CDR server
CSV	`file:disk`	Disk can be any name, as it is not used by the program anyway.
Email	`mailto:name@company.com`	

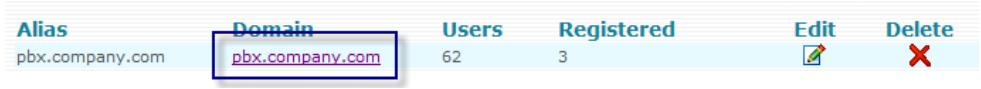
- **Record Location:** This field determines where system-initiated recordings will be stored on the system. By default, `$r/$o/$a/$d-$t-$i-$n.wav` is the string used in this field. For more information about recording calls and how to create a string for the **Record Location** field, see page 315294.
- **Compress Recording:** The system will compress recordings when this setting is enabled. Otherwise, recordings will be saved as 16 bits/sample.

- **Hide aliased rows under domains page:** This setting allows you to control whether the alias account of your domain will be displayed on the Domains page. When this setting is set to **No**, the list of domains will include the alias in addition to the primary domain, which may be confusing since it appears that more domains are on the system than there actually are. When this setting is set to **Yes**, only the primary domain(s) will be displayed.

  Before (set to No):

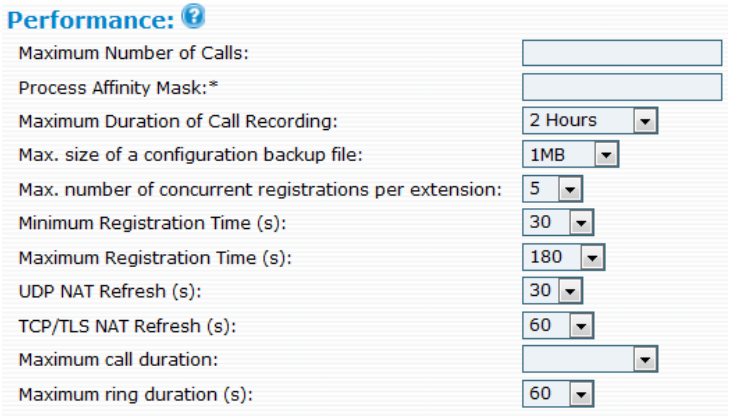


  After (set to Yes):



Performance

From this section, you can set performance-related settings.



- **Maximum Number of Calls:** This setting defines the number of simultaneous calls allowed by the system. Because every call requires a certain portion of the available CPU, allowing too many calls will affect the quality of all ongoing calls. By limiting the number of calls on the CPU, you can reject calls

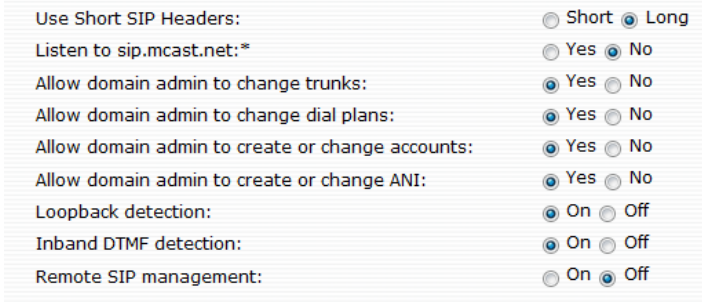
that would otherwise potentially degrade overall performance. On modern PCs, 100 or more calls can run on one computer; however, on an embedded system, you will probably have much less CPU power and thereby increase the probability of running out of CPU power if you allow that many calls. If this field is left blank, the key in the system will limit the calls, or the CPU limitation, when reached, will limit the calls.

- **Processor Affinity Mask:** This field allows the administrator to assign a particular CPU to the pbxctrl system process. When using a multiple-core CPU, the operating system has to assign processes to processors. By default, the operating system tries to balance out the load so that the overall system performance is as fast as possible. However, the disadvantage with this approach is that the whole process gets stuck for some time while moving the processes from one CPU to another. If during that time the CPU should play out media, it will come across as stuttering and be perceived as jitter coming from the system. In order to avoid this problem, bind the pbxctrl to one fixed CPU. Depending on the operating system, you can do this manually or you can ask the system processes to do this during startup. Changes to this field require a system restart.
- **Maximum Duration of Call Recording:** This setting allows you to establish an upper limit on call recordings, which is important since large recordings can cause problems with system performance. To further conserve on disk space, you can limit the number of messages that can be stored in a user's voicemail box (see the **Voicemail Size** setting on page 98).
- **Max. size of a configuration backup file:** This setting allows you to establish the maximum size, in bytes, of the backup file. The default is 1 MB. If your system has a lot of data to be backed up, increase this value. The backup feature through the web interface is used mostly in the appliances (in embedded systems where the file access is primitive). On other systems, it is advisable to use the OS file manager to do the backup.
- **Max. number of concurrent registrations per extension:** This setting controls how many user agents (i.e., phones) can be registered against an extension. This feature is useful if you want to restrict the number of phones that can be registered to an extension. If this field is left blank, the extension will have no limit.

- **Minimum Registration Time (s):** In a SIP environment, the registrar determines how long a user agent may be registered. Short registration times have a negative impact on the performance; however, it is critical that user agents stabilize quickly once they've lost their connection to the system. This setting defines the lower limit for the registration time. The default is 30 seconds.
- **Maximum Registration Time (s):** This setting is used to define the upper limit for the registration time. The default value is 360 seconds. See also Appendix B, "SIP Overview."
- **UDP NAT Refresh (s):** If the registering user agent is behind NAT, the system uses this setting to control the registration. The system registers agents that use the UDP transport layer only for a short time so that the user agents will re-register quickly and keep the NAT bindings alive. Typically, the settings for UDP should be from 15 to 45 seconds since most NAT routers close ports after 60 seconds of inactivity. The default for this setting is 30 seconds.
- **TCP/TLS NAT Refresh (s):** This is similar to the UDP NAT refresh setting. Since TCP/TLS connections do not need to refresh the bindings as often, a value of a few minutes is okay in most situations. The default is set to 180 seconds (3 minutes).
- **Maximum call duration:** This setting establishes an upper limit for the call duration. By default, the setting is 2 hours (7200 seconds), but you can increase this setting if you lean toward longer phone calls. This setting is crucial for keeping your call list clean; for example, if one mailbox talks to another mailbox or if a call does not drop properly, the system can automatically clean this up.
- **Maximum ring duration (s):** This setting determines the length of time the system will wait before it disconnects a call.

SIP Settings

This section defines SIP-related settings.


Use Short SIP Headers: Short Long
Listen to sip.mcast.net:* Yes No
Allow domain admin to change trunks: Yes No
Allow domain admin to change dial plans: Yes No
Allow domain admin to create or change accounts: Yes No
Allow domain admin to create or change ANI: Yes No
Loopback detection: On Off
Inband DTMF detection: On Off
Remote SIP management: On Off

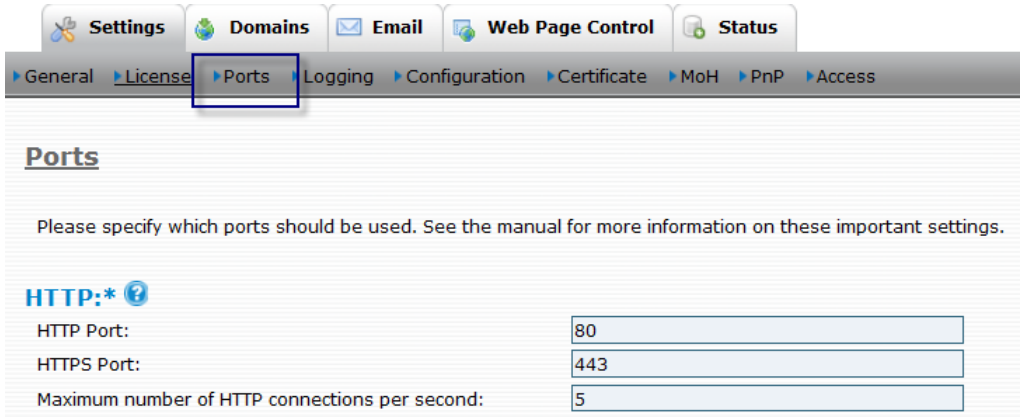
- **Use Short SIP Headers:** Some SIP headers have a short form (e.g., the `From` header gets shortened to `F`, the `To` header becomes `T`, and `Via` becomes `V`). Short headers have the advantage of saving space in the messages, reducing overall probability of running into problems with maximum message size in UDP. Although it is quite simple to support this, some devices do not support short headers. For this reason, the system offers both short and long. To maximize interoperability, keep the default value (long). If you are running into UDP packet fragmentation problems (message size above 1492 bytes), switch to the short header form.
- **Listen to sip.mcast.net:** SIP has its own multicast group according to RFC 3261. A SIP device usually knows where to send requests, but during bootup and configuration, a user agent might want to locate the system with a multicast request. If this setting is turned on and you are using user agents with the multicast detection feature, you can just plug the devices into the network and they will get their configuration information automatically from the system if the system PnP settings have been configured (see Chapter 20). Changing the **Listen to sip.mcast.net** setting requires a system restart.
- **Allow domain admin to change trunks:** In hosted environments, the service provider might want to set up the trunks and then hide them from domain administrators. When this feature is set to **No**, domain administrators will be unable to edit or view trunks.

- **Allow domain admin to change dial plans:** This feature allows the administrator to hide all dial plans from domain administrators. When this feature is set to **No**, domain administrators will be unable to change or view dial plans.
- **Allow domain admin to create or change accounts:** If this feature is set to **No**, domain administrators cannot create, change, or view accounts.
- **Allow domain admin to create or change ANI:** If this feature is set to **No**, domain administrators cannot create or change the ANI (automatic number identification). The ANI is used when the system sends an outbound call on a trunk (see page 95 for more information on the default ANI).
- **Loopback detection:** This setting applies only to multi-domain environments (for single-domain environments, leave this setting on). When the system starts a call, that same call may come back to the system and create a loop. This may happen if the call is made to another caller on the system in a multi-tenant environment. This is a dangerous situation because it might repeatedly initiate the same call, ending up in many calls that take a lot of resources. Therefore, the system must detect such a loop. In environments where an external SIP proxy routes the call from one snom ONE domain to another, a simple loopback detection that is based on the call-ID is too pessimistic. Therefore, in such environments, you might want to allow these calls and turn the loopback detection off (see the **Try Loopback** setting on page 155).
- **Inband DTMF detection:** When a user presses a key on the telephone, the system must be able to understand the action. In telephony systems, this mechanism is typically called DTMF. In VoIP, DTMF is usually sent "out of band" (RFC 2833) because it allows the system to easily detect the tones in a fail-safe manner. However, not all devices support this method, and when this is the case, the system must decode and analyze the media stream and perform this detection. Because this is erroneous and costs additional CPU performance, it is strongly recommended that you not use this feature and instead replace devices which do not support the out-of-band method with devices that do. In-band and out-of-band can be compared to a T1 line that uses in-band signalling and a PRI line that uses out-of-band signalling.
- **Remote SIP management:** This setting allows the provider to send commands to the system (for example, for rereading the configuration). It is useful in environments where the service provider controls the system from a central-

ized location. By default, this setting is off, but if your network is in such an environment, this setting needs to be activated.

Ports

The Ports page allows you to control which networking resources the system will utilize when communicating with the outside IP world. When specifying ports, list the ports that you may bind to, either specifying a port number or explicitly specifying the IP address and the port, separated by a colon (e.g., `192.168.1.2:8080`). If you are binding to IPv6 addresses, place square brackets around the IP address, e.g., `[2001:db8::4]:5060`. If you are specifying only the port number, the system will bind to all IPv4 and IPv6 addresses on the system. If you want to bind only to IPv4 sockets, use the form `0.0.0.0:5060`. If you want to bind only to IPv6 sockets, you can use `[::]:5060`. In general, you may bind to more than one socket; just separate the addresses by spaces. If you do not want to use the service, leave the field empty. If you change a port binding, you will need to restart the snom ONE service. We support the default SIP port.



* Changes to HTTP and SIP settings require a system restart.

HTTP Ports

The HTTP and HTTPS ports are used to communicate between the built-in web server and the web browser (snom ONE does not rely on IIS or Apache for its web

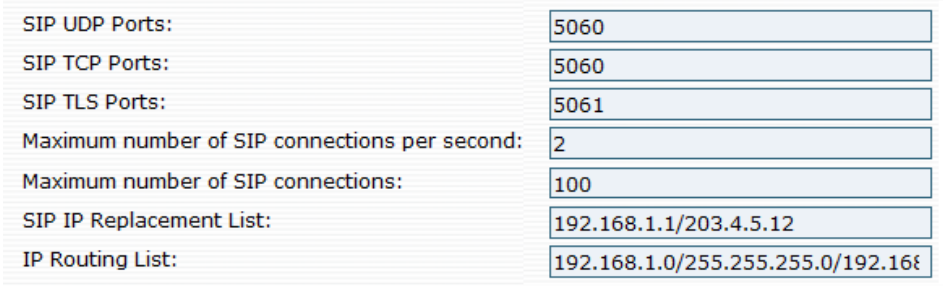
interface). The HTTP port is used for insecure, but lightweight, communication. The HTTPS port is used for communication that is secure, but a bit more expensive.

If you cannot reach the system on any port, change the *ip_http_port* and *ip_https_port* parameters in the global configuration file (the defaults are shown below). If you are running another service on your host or if you want to gain some additional security, you may change these ports to any other available port. The system will fail to start if it cannot bind to the port.

- **HTTP Port:** The default HTTP port is `80`.
- **HTTPS port:** The default HTTPS port is `443`.

SIP Ports

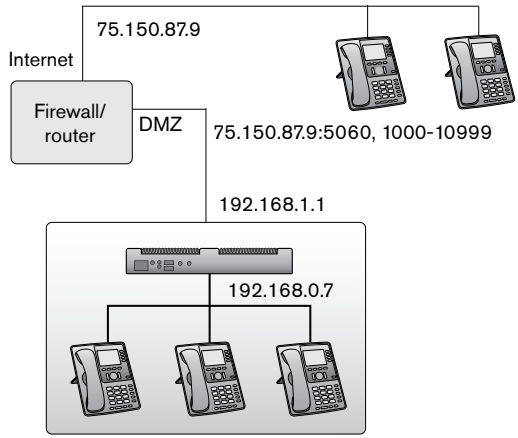
In this section, you can provide specific port information for the SIP protocol. SIP can run on UDP, TCP, or TLS. TCP and UDP send the SIP packets unencrypted and are therefore considered insecure. TLS is used for secure SIP communication since it encrypts the SIP signalling packets much like HTTPS encrypts HTTP traffic. The default SIP port per RFC 3261 is 5060 for SIP and 5061 for SIPS. The snom ONE software is listening for and transmitting SIP requests and responses on these ports.



* Changes to HTTP and SIP settings require a system restart.

- **SIP UDP Ports:** If you are using SIP over UDP, you need to set this field. The default port for UDP is `5060`, but multiple ports are permitted (e.g., `5060 5064`).
- **SIP TCP Ports:** If you are using SIP over TCP, you need to set this field. The default port for TCP is `5060`.

- **SIP TLS Ports:** If you are using SIP over TLS (Transport Layer Security - Security over TCP), you need to set this field. The default port for TLS is `5061`.
- **Maximum number of SIP connections per second:** This setting specifies the number of SIP conversations the system will respond to in 1 second. This setting is useful for deterring against SIP attacks.
- **Maximum number of SIP connections:** This setting limits the total number of SIP connections the system will support. This setting must be configured in busy environments where resource limitation is an issue.
- **SIP IP Replacement List:** This setting applies to a system that is used in a DMZ zone with NAT (e.g., for remote phones that are connected to a system which is not on a public IP address). In this case, when the system builds the remote SIP packets, it will use the public IP address of the router. The setting should include a list of local IP addresses and their replacements (e.g., `192.168.1.0/255.255.255.0/192.168.1.1 0.0.0.0/0.0.0.0/75.150.87.9`). Whenever the system finds a local address in the list, it replaces the local address with the remote address, so the SIP messages from the system will look as if they were sent from the replaced IP address. The format of the list is LocalAddress/RemoteAddress [LAdr/RAdr]. Both the LAdr and the RAdr must be an IPv4 or IPv6 address (e.g., `192.168.1.2/203.4.5.12`). DNS addresses are not resolved here.



- **IP Routing List:** The **IP Routing List** setting is used to override the operating system IP routing table and is linked to the routing table (this setting will

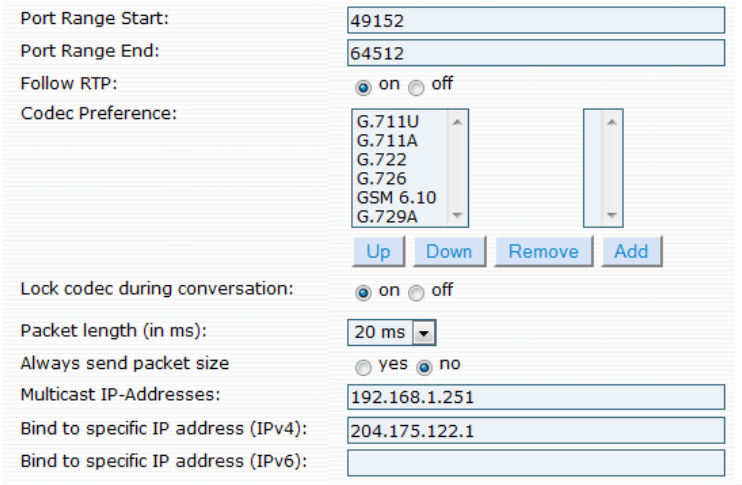
be consulted by the system before consulting/using the operating system). Whenever the system wants to find the IP address that is being used when sending a SIP packet, it steps through the list and looks for a match (using the netmask mask) to a destination address (DAdr). If a match is found, the system uses the provided IP address (LAdr). The mask must be in the form of an IP address, e.g., `255.255.255.0`.

RTP Ports

The Real Time Protocol (RTP) ports are used for sending and receiving media. Be sure to specify a reasonable port range so that you have enough ports for all open calls. A port range of 100 ports is not unusual.

Most user agents send RTP media data from the same port on which they expect to receive data. This is useful when a user agent sends media from behind NAT. The system can use this mechanism to establish a two-way media path, even if the user agent is not able to determine its public IP address for media and is behind NAT.

- **Port Range Start:** This setting represents the starting RTP port that the system will use for media sessions. If the system is behind a firewall, these ports should be open.
- **Port Range End:** This setting represents the end RTP port that the system will use for the media sessions. RTP uses UDP for transport, whereas SIP can use UDP, TCP, and/or TLS.



- **Follow RTP:** Some user agents use different ports for sending and receiving. Although they will not be able to operate behind NAT, they are within the scope of the IETF standards. With this setting, these devices can be made compatible. By default, this flag is set to **on**. If you have trouble with devices that use different ports for sending and receiving, try turning this flag off. (If this setting is already set to **off** and you are still having trouble, try turning it on.) Some troublesome devices also have a flag that can be used to turn the usage of different ports off.

  This behavior can also be controlled on a trunk level, so if only a specific trunk has this problem, use this setting only on the trunk level.

- **Codec Preference:** The **Codec Preference** setting allows you to select the codecs that will be supported on the system. The codecs that are allowed on the system are shown at the left. If you do not want to use a particular codec, click the codec, then click **Remove**. This will move the codec to the right-side selection box, removing it from use. The system comes with recommended high-quality codecs like G.711 µ-law (0), G.711 A-law (8), G.722 (9), G.726 (2), or GSM 6.10 FullRate (3). Codecs can be changed without restarting the service. G.729 is a royalty-based codec and requires a fee (it is not enabled by default). If you don't have any bandwidth constraints, you can use G.711. If bandwidth is a concern, you should look to compress the data using an LBR (low bit rate) codec.

- **Lock codec during conversation:** In certain cases, the system can switch to a common codec (advertised by both end devices) to avoid the transcoding during the call setup. Even though this is legal from the protocol's point of view, many devices still cannot change codecs midstream. To avoid this problem, you must enable this feature.

  Once this is set, the system will not switch the codec during the call setup. This may introduce transcoding, which is a CPU-intensive job. Default is off.

- **Packet length (in ms):** This is the `ptime` parameter in the session description protocol (SDP). The default is 20 ms.

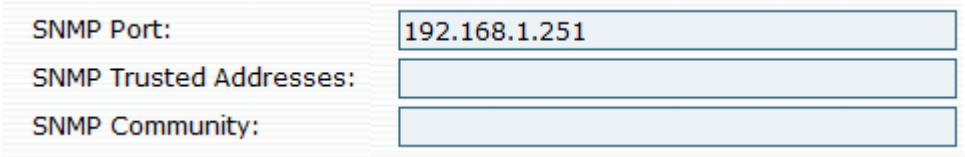
- **Multicast IP Addresses:** Set this to an IP address if you want the system to send and receive multicast IP addresses on this network interface. If this is set to 20 ms, then the system will send out packets every 20 ms, which equals 50

packets per second. If both sides of the call are set to different ptimes, then the system will have to transcode them, which will degrade performance.

- **Bind to specific IP address (IPv4):** The system listens to SIP requests that are sent by the user agent from this IP address only. This is useful if you have a dual NIC machine and want to listen to SIP requests only on one interface. If this is left blank, then the system will listen to SIP requests on all interfaces it sees in the machine.
- **Bind to specific IP address (IPv6):** The system listens to SIP requests that are sent by the user agent from this IP address only.

SNMP

Simple Network Monitoring Protocol (SNMP) is used to poll the system for information. Table 2-5 lists the information that can be made available to an SNMP management tool.



- **SNMP Port:** The SNMP port setting defines the port on which the system will listen for SNMP requests. By default, the port is 161.
- **SNMP trusted addresses:** This field lists the IP addresses that may send SNMP requests. If this setting is empty, the system will not accept any SNMP requests. Whenever a request is rejected, the system writes a log message. This field requires the IP address of the SNMP server.
- **SNMP Community:** An SNMP community is the group to which devices and management stations running SNMP belong. If you would like to change the community, you can do so from the web interface. It does not require a restart of the service. SNMP default communities are private (write) and public (read). The system, by default, is set to public.

Table 2-5. Available SMNP Sensors

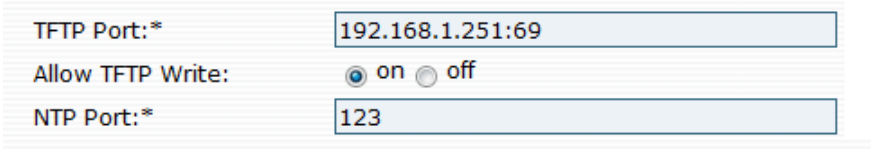
OID	Description	Absolute	Unit
1.3.6.1.4.1.25060.1.1	Call legs	Yes	Calls
1.3.6.1.4.1.25060.1.2	Registrations and subscriptions	Yes	Registrations
1.3.6.1.4.1.25060.1.3	Messages	Yes	Minutes
1.3.6.1.4.1.25060.1.4	Call attempts	No	Calls
1.3.6.1.4.1.25060.1.5	Successful calls	No	Calls
1.3.6.1.4.1.25060.1.6	Media CPU load	Yes	Value 0..100
1.3.6.1.4.1.25060.1.7	Successful emails	No	Emails
1.3.6.1.4.1.25060.1.8	Unsuccessful emails	No	Emails
1.3.6.1.4.1.25060.1.9	Email alert flag	Yes	Value 0..1
1.3.6.1.4.1.25060.1.10	SIP received packets	No	Packets
1.3.6.1.4.1.25060.1.11	SIP sent packets	No	Packets
1.3.6.1.4.1.25060.1.12	Allocated memory	Yes	Bytes
1.3.6.1.4.1.25060.1.13	Calls	Yes	Calls
1.3.6.1.4.1.25060.1.14.x	Trunk calls	Yes	Calls
1.3.6.1.4.1.25060.1.15.x	Trunk status	Yes	SIP response code
1.3.6.1.4.1.25060.1.16	Uptime	Yes	Seconds
1.3.6.1.4.1.25060.1.17	Disconnects (no media)	Yes	Calls
1.3.6.1.4.1.25060.1.18	Disconnects (media timeout)	Yes	Calls

TFTP

The TFTP ports are used for provisioning purposes. Many SIP devices use TFTP for automatic configuration.

- **TFTP Port:** The TFTP (Trivial File Transfer Protocol) port is on port 69 by default. If your machine has multiple network interface controllers (NICs), you may specify the IP address port to bind only to that port.
- **Allow TFTP Write:** Some devices write log files using TFTP, which can be enabled with this feature; however, keep in mind that this feature enables users

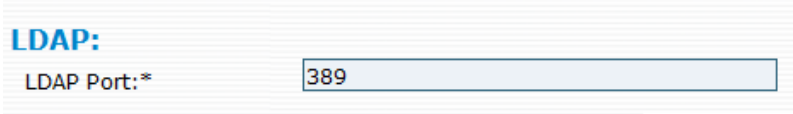
to write files that affect other devices, and this may introduce system instability and security concerns. Per the example above, you can also bind to a private IP address, which will make it more secure.



- **NTP Port:** The system can act as an NTP (Network Time Protocol) server for the network. If you want to run the NTP server on the system, use this field to provide a port number on which it can run. By default, the **NTP Port** field is blank so that the system doesn't respond to NTP requests. The default port is 123, so if you populate it and restart the service, the system will respond to NTP. The phone gets its time from the NTP, so if the phone cannot reach the Internet, then a local NTP server is necessary. A popular, publicly available NTP server is pool.ntp.org.

LDAP

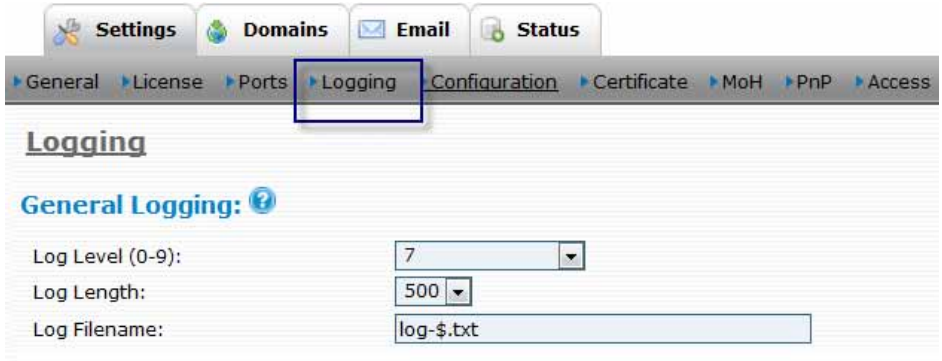
LDAP (Lightweight Directory Access Protocol) is an Internet protocol used to access directory type of information, such as address books. All snom phones support LDAP, so users can query phone numbers by pressing the directory button of the phone. LDAP makes it easier for companies to share a common directory.



- **LDAP Port:** Port 389 is the default port.

Logging

Logging is a powerful mechanism for tracking system activity. Once you have installed the system, the logging feature allows you to see how it works and how the system interprets the input to the system.



General Logging

- **Log Level (0-9):** This field determines which log messages are included in the log. The range is between 0 and 9. Level 0 will show you only critical messages, while level 9 will show you every available log messages of the system. Log level 9 should be used only for troubleshooting, as it creates additional load for the system and may generate extremely large log files.
- **Log Length:** This setting determines the length of the internal log message buffer and is used to show the log messages in the web interface.
- **Log Filename:** To request that the system write log messages to a filename, specify that filename here. If you enter a dollar sign into the log filename (highly recommended), the system will replace the dollar sign with the current day and automatically generate a new file everyday. This will ensure that the log files do not become too large over time. It is highly recommended that you *not* log to a file without using the dollar sign. Also, be sure to delete old log files from time to time so that your file system does not get overloaded with too much logging information.

  One of the first log messages that you will see will be in the working directory. If the **Log Filename** setting does not contain a path, the system will write the log file to that directory. You can specify the directory during the installation process.

  Example: The setting `log-$.txt` will create a log file under the system working directory with the name `log-yyyy-mm-dd.txt`, where `yyyy` is

the year, `mm` is the month, and `dd` is the date. If you have multiple drives, it is good practice to write the logs there (e.g., `D:\logs`).

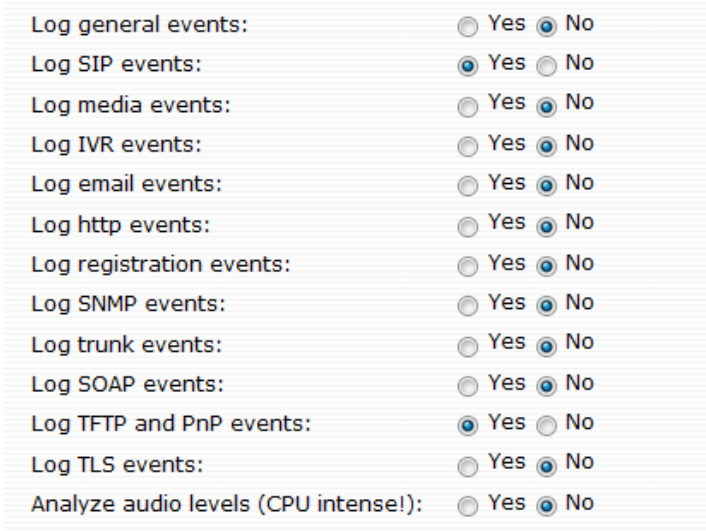
Warning: Please note that using a log file without a dollar sign as part of the name is a ticking time bomb. While the system may initially run fine, system instability is likely to occur as disk space becomes consumed.

Warning: Be sure to lower the log level once the system is running, especially when you write the log messages to a file. Sooner or later, you will get a hard disk full error, which is a severe situation because the system will not be able to save runtime data.

Specific Events

You can enable or disable logging on a subsystem level (available subsystems are shown below):

- **Log general events:** These events are of general interest, for example, information about the working directory.
- **Log SIP events:** Events in this module relate to the SIP traffic of the system.
- **Log media events:** The system reports events about media processing, for example, a one-way audio RTP timeout.
- **Log IVR events:** This module logs events related to processing user input (e.g., all DTMF events, including the auto attendant and the mailbox).
- **Log email events:** If you want to troubleshoot the email server interaction, turn this module on so that you'll see SMTP events.
- **Log http events:** This flag controls whether events in the internal HTTP server should be logged.
- **Log registration events:** When a device registers or deregisters, it appears in this module.
- **Log SNMP events:** SNMP events occur when an external SNMP agent requests information from the system (see also page 58).
- **Log trunk events:** Log events are related to trunks (e.g., when a trunk registers for the first time or when an inbound trunk calls).


Log general events: Yes No
Log SIP events: Yes No
Log media events: Yes No
Log IVR events: Yes No
Log email events: Yes No
Log http events: Yes No
Log registration events: Yes No
Log SNMP events: Yes No
Log trunk events: Yes No
Log SOAP events: Yes No
Log TFTP and PnP events: Yes No
Log TLS events: Yes No
Analyze audio levels (CPU intense!): Yes No

- **Log SOAP events:** This subsystem deals with SOAP input and output.
- **Log TFTP and PnP events:** This module includes events related to the built-in TFTP server. It also includes information related to plug and play.
- **Log TLS events**: This module logs TLS-related messages in the log file.
- **Analyze audio levels (CPU intense!):** This feature measures the audio levels on a call leg. The volume is measured in decibels (dB) relative to the maximum volume (0 dB is maximum loudness).

SIP Logging

Logging is important when tracking down problems. The settings on this page are designed to help you troubleshoot.

SIP Logging:
Log REGISTER: Yes No
Log SUBSCRIBE/NOTIFY: Yes No
Log OPTIONS: Yes No
Log Other Messages (e.g. INVITE): Yes No
Log Watch List (IP):
Log Watch List: 7

When the system receives or sends a SIP packet, it determines whether the packet will be logged and which log level the event will have.

- **Log REGISTER:** REGISTER packets deal with the registration of extensions or trunks, which can generate a lot of traffic. If you are not interested in the registration traffic, disable this setting (see Appendix B for more information on SIP messages).
- **Log SUBSCRIBE/NOTIFY:** SUBSCRIBE/NOTIFY deals with message waiting indications (MWIs), the LED state, and other used subscriptions.
- **Log OPTIONS:** OPTIONS can be used to keep the SIP connection alive. They are designed so that a user agent can see which options or methods the other user agent supplies. OPTIONS allow you to view the full SIP messages with all the SIP header information (when using log level 7).
- **Log Other Messages (e.g., INVITE):** All other packets usually belong to an ongoing call (e.g., INVITE, CANCEL, ACK, BYE).

When you enable the logging for one of the previous categories, the SIP packets will be logged on log level 7. If your log level is below 7, the packets won't show up in your log.

- **Log Watch List (IP):** The watch list filters the SIP packets by IP address. This feature is useful when you have a specific device that you want to watch in the system's log. Enter the IP addresses into this field.
- **Log Watch List:** This setting defines the log level for the previous setting—Log Watch List (IP). The log level for the watch list is independent of the log level of the packets that are not on the list (and which are on level 7). This makes is possible to lower the log level and show the SIP packets of a specific device also on a lower log level.

  Example: If you want to log SIP messages from 192.168.1.113 only, configure the following settings:

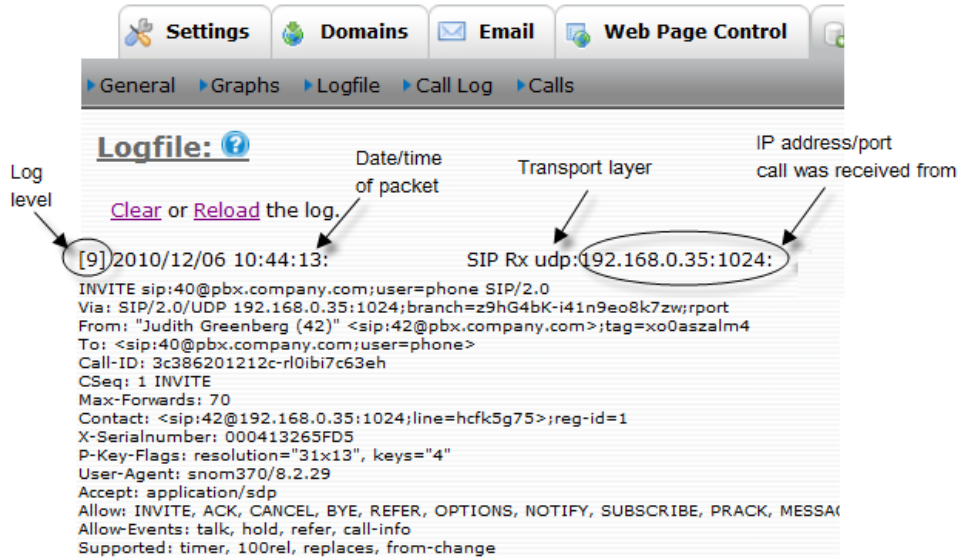
  - Log Watch List(IP): Set the IP address (e.g., 192.168.1.113).
  - Log watch list: 7
  - Log Level: 8
  - Specific Events: Enable Log SIP events. This filters out all the events, since they are set at 8 and log watch is set at 7.

  Turn off everything under SIP Logging.

Retrieving SIP logging

The SIP log is the most common logging that is requested. Use the following steps to turn on SIP logging:

1. Navigate to **Admin** > **Settings** > **Logging**.
2. Set Log Level to `7`.
3. Set Log Length to `300`.
4. Under "Specific Events," enable the following settings:
   - Log general events
   - Log SIP events
   - Log trunk events
5. Under "SIP Logging," enable Log Other Messages (e.g., INVITE).
6. Click **Save**.
7. Navigate to **Admin** > **Status** > **Logfile**, and click **Clear**. This will clear the page.
8. Make the call.
9. Navigate to **Admin** > **Status** > **Logfile**, and click **Reload**.



Configuration

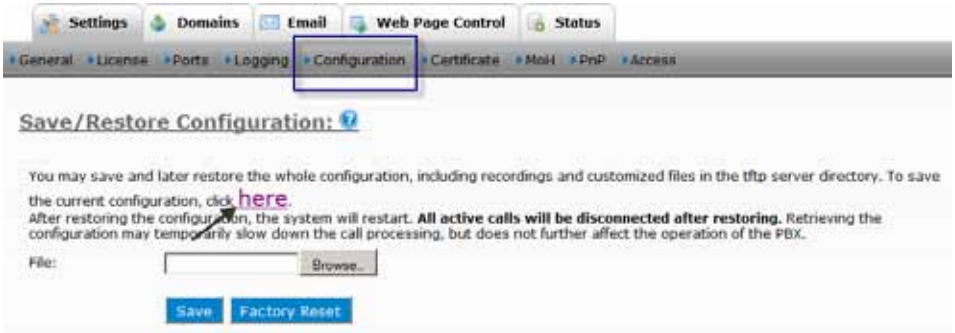
This section shows you how to save and restore the system configuration, as well as load the configuration XML files. This will generate a complete backup of your system, including all temporary files, recordings, TFTP server files, etc. You can even schedule this task nightly so that you automatically have a fresh backup for disaster recovery.

Important: The backup from the web interface is designed for smaller systems. If the working directory of the system is larger than 5 MB, it is best to use TAR or ZIP and move the backup to another storage place.

Save/Restore a Backup

This backup will make a TAR backup of the whole configuration, including audio recordings. Because the file might get potentially large, you should perform this action in times when there is not too much going on in the system. This will prevent you from interfering with the service and will ensure that you get an integer snapshot of the system state.

1. Use the "click **here**" link, as shown in the following image.


Settings
Domains
Email
Web Page Control
Status
General
License
Ports
Logging
Configuration
Certificate
MoH
PnP
Access
Save/Restore Configuration:
You may save and later restore the whole configuration, including recordings and customized files in the tftp server directory. To save the current configuration, click here.
After restoring the configuration, the system will restart. All active calls will be disconnected after restoring. Retrieving the configuration may temporarily slow down the call processing, but does not further affect the operation of the PBX.
File:
Browse...
Save
Factory Reset

2. When prompted, save the file on the local computer.

Important: The size of the file is limited by the **Max. size of a configuration backup file** setting (see page 49). If the TAR file exceeds the configured size, the backup will fail and an empty file will be returned. Therefore, be sure to check whether the file size is okay after storing the backup. If there is a problem, consider making the file system backup manually.

To restore the backup

To restore a configuration, the file must be loaded through the web interface. As with saving the configuration, this may be time-intensive, so be sure to do this when no calls are on the system. The system restoral will first erase your existing configuration, so exercise caution with this step.

1. Click **Browse** to find the file to be restored (the full path of the file is required). This file is the one you backed up in the previous section.
2. Click **Save** to load the selected file. This will load the selected file, and the system will have the new configuration.

Warning: The **Factory Reset** button will load a default configuration file from the file system. All data will be erased.

Note: The global parameter (`max_tcp_length`) can accommodate the large TAR files. You will need to set this before running the backup/restore. Currently, this value is in bytes, so you will need to provide a value similar to 384000000 (for 384 MB).

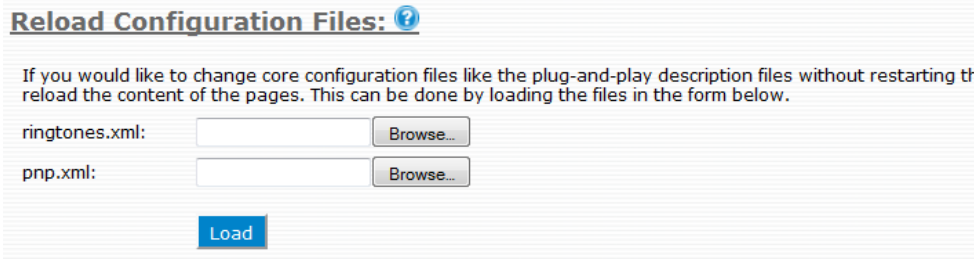
Request Configuration

The system may receive its configuration information from a service provider. Be especially careful when using this feature because it may overwrite your existing configuration without further warning. If you leave the URL empty, the system will use the default URL. Please note that your license key will be sent over the Internet (encrypted).

If you have a web service that generates configurations dynamically, you can request the pull-down of a configuration from the web server. The system will initiate the web request on its own. This feature is useful in large-scale installations (many systems running as CPE devices) that involve a central configuration management database.

Reload Configuration Files

Configuration files `ringtones.xml` and `pnp.xml` can be customized for your system. These files can be downloaded from wiki.snomone.com and uploaded through the **Browse** option shown below. You can also place the files into the `html` folder and restart the system (downloads are available at wiki.snomone.com). See also “Customized Ringtones” on page 323.

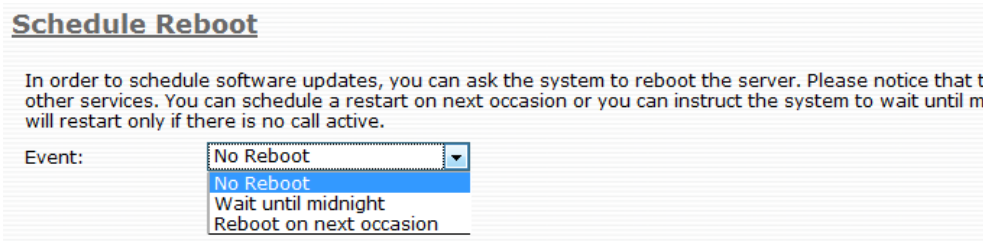

Reload Configuration Files:
If you would like to change core configuration files like the plug-and-play description files without restarting th
reload the content of the pages. This can be done by loading the files in the form below.
ringtones.xml:
Browse...
pnp.xml:
Browse...
Load

The files are detailed below:

- `ringtones.xml`: This file is used to describe the available `Alert-Info` or `Call-Info` header that should be sent in the different `Alert-Info` headers. Some phone vendors handle these headers differently, and this file can be used to address that.
- `pnp.xml`: This file is used to describe the files that are available for plug and play. This file also defines various parameters for different phone models and vendors (see Table 20-3).

Schedule a Reboot

To schedule software updates, you can request that the system reboot the server. (This applies to non-Windows servers only.) Note that during a reboot, all services will be shut down. You can schedule a restart on the next occasion, or you can instruct the system to wait until midnight. In any case, the system will restart only if there is no call active.


Schedule Reboot
In order to schedule software updates, you can ask the system to reboot the server. Please notice that t
other services. You can schedule a restart on next occasion or you can instruct the system to wait until m
will restart only if there is no call active.
Event:
No Reboot
No Reboot
Wait until midnight
Reboot on next occasion

Certificates

Digital certificates are electronic documents that are used to verify that the system you are interacting with is legitimate. The system can support multiple certificates, which allows you to have a certificate for each domain. The PBX uses certificates in multiple ways:

- For securing the traffic between the web browser and the web interface of the system when HTTPS is used.
- For securing the SIP traffic between the phone and the system's signaling path when TLS is used.
- For your email server when it requires TLS (e.g., gmail).

When using certificates on snom ONE, you can choose from the following four types:

1. Domain certificate chain + private key: While "Server certificate chain + private key" is the default for the whole server (see below), the PBX can also present domain-specific certificates that require that the client, at the beginning of the session setup, tell the server which domains it wants to connect to. With this type of certificate, the domain name must be in the certificate, as the PBX uses it during the import process.
2. Server certificate chain + private key: The PBX also needs to present a certificate when it is being connected to. In this case, it must also have a private key associated with it. The certificate portion may actually consist of a certificate path so that the caller can verify where it comes from.
3. Trusted Root CA for server authentication: This certificate is used by the snom ONE built-in web client when assessing whether or not it can trust the server it is connecting to.
4. Trusted Root CA for client authentication: This certificate is used for client certificate authentication and is needed essentially when a phone requests provisioning. This way, the PBX can be sure that an actual phone is downloading the configuration and not a hacker using a web browser.

Getting a Valid Certificate

Buying a Certificate

When you buy a certificate, it must be known that you are really the one who is operating a server. Although the mechanisms for this process differ, all services require that you pay for the service and that your web browser is already set up to trust the certificate authority. This mechanism is suitable if you are operating a public service where it is not an option to load root certificates on many clients. You usually also need to specify which IP addresses are using this certificate for the service.

Making Your Own Certificate

You also have the option to generate your own certificates if you have control over the clients. For example, you can join the community at http://cacert.org and generate them there. You will need to load the root certificate into the clients that should talk to the snom ONE system.

There are various other sites available which provide a similar service. You may also download the openSSL toolkit and compile your own certificate generator and set up your own trusted network. If you have already done this to secure your other office infrastructures (e.g., email or VPN), you can probably reuse those certificates.

Certificate Size and Format

Please use only 512 and 1024 bit certificates. The system currently has trouble handling certificates with other sizes. The security and the performance on these certificates is still reasonable.

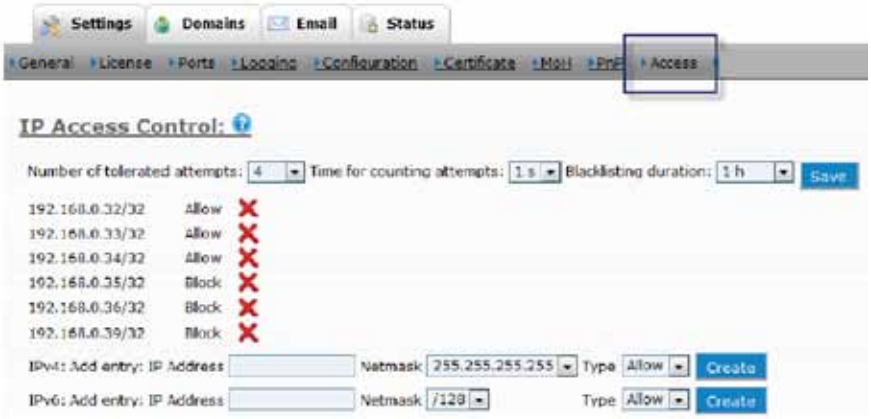
The format of the certificate must be base64-encoded. You must include the private key and the certificate in the upload. Please note that uploading the private key this way might be intercepted by an intruder. You can minimize this risk by using the localhost address from the local machine.

In order to provide the key, just enter the ASCII string that you received from the trusted party, copy it into the text field, and press **Save**. The system will then present this certificate to HTTP and SIP connections that require secure communications.

Access List

If your system is under a denial of service attack, the system will automatically block the IP address that is attacking the system. You can also add IP addresses to the **Access** page and place a **Block** on them so that they will be unable to access the system. Just enter the IP address, the net mask, and the access type, and click **Create**. Enter only as much information as needed by the net mask; for example, if the net mask is "255.255.0.0," enter `192.168.0.0`. To delete an entry, click the **Delete** button.

Changing the entry does not require a restart of the system. The changes take effect immediately.



You may specify IP addresses with their netmask and their policy. If no match is found, packets will be accepted. System administrators might want to define who has access to the system for a number of reasons:

- Protection against denial of service attacks: If you are operating the system on publicly available addresses, there is always the risk that someone will try to interrupt the service. Although the system has several protections against such attacks, it might be easier to rule out such attacks from the beginning.
- Limiting the service to authorized addresses: You might also want to limit the service to specific IP addresses only. For example, while you might allow users to register their IP phones in the office, you might allow only selected users with their associated IP addresses to register their phones from home.

The motivation for the list is to provide the firewall type of functionality within the system application and reduce the chance of unauthorized access to the system.

The access control is not limited to SIP only, but it also applies to all other protocols on the system, including HTTP, TFTP, and SNMP. When the system acts as a client (for example, when performing DNS requests), the rules do not apply. Using 0.0.0.0 in the IP field specifies that everything will be accepted. In addition, if you are getting a lot of requests from a particular source, the system will automatically add them to the access control list and block them.

How the Access List Functions

When a packet reaches the system, the system checks the list of enabled and disabled addresses for a match. If the request is ignored, the system discards the packet without answering. When the system checks the list for matches, a match occurs if a "source address" matches a "check address" with the mask. More specific addresses are checked first, making it possible to define exceptions to the general rule. Also, the system checks IPv4 and IPv6 addresses separately. If there is a match, the system checks for the type. If the type is **Allow**, then the system accepts the packet. If the type is **Block**, then the system blocks that request. If there is no match in the list, then the request is accepted. If the list is empty, the access control is disabled. This is the default behavior after the installation of the product.

For UDP-based requests, this is relatively easy—the request is just not answered. But because the UDP port is open, there is no ICMP request sent to the origin, which means if someone wants to attack the system, it might be possible for the attacker to figure out that there is an open port. But since the system just discards these messages, the damage is limited.

For TCP ports, the situation is more complicated. In Linux, there is no way for an application to determine where a TCP connection is coming from until the connection is accepted. This is why the system first accepts the connection and then examines whether the connection was allowed or not. If the connection was not allowed, then it is turned down immediately. In Windows, there is a special system call that first checks where the connection is coming from. If the source is not enabled, then the system does not accept the connection. However, because the operating system has already answered the TCP connection request with an acknowledge, in Windows it will be obvious that an application is running on the ports.

The behavior of the access list is similar to a firewall. However, especially for TCP, a firewall will keep the traffic completely out. Someone testing the system will not get a response for a TCP request if the source IP address is not listed.

Example

Table 2-6 shows a scenario in which all users in the LAN are given access, but access from the public Internet is not allowed, except for two employees working from home and a trunk that comes from a service provider with a small range of IP addresses.

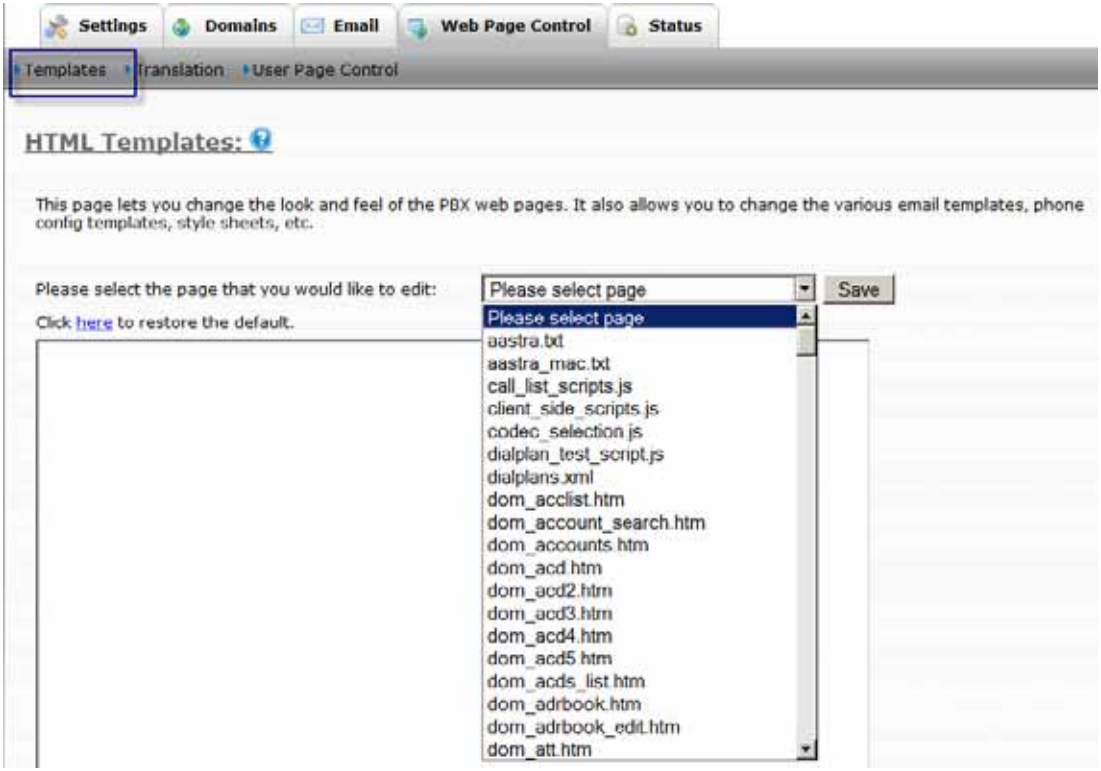
Table 2-6. Access List Scenario

	Address	Net Mask	Type	Description of Result
First entry	127.0.0.1	255.255.255.255	Allow	This entry will ensure that you can always access the HTTP interface from the local computer.
Next entry	192.168.0.0	255.255.0.0	Allow	This entry will ensure that everyone in the LAN can access the system.
Next entry	0.0.0.0	0.0.0.0	Block	This entry will disable all packets by default. Populate this entry last; otherwise, you will be unable to access the system.
Next entry	213.1.2.3	255.255.255.255	Allow	This entry will give the remote worker access to the system. Repeat the same entry for other IP addresses.
Next entry	12.23.34.45	255.255.255.248	Allow	This entry is intended for the IP addresses of the ITSP.

Web Page Control

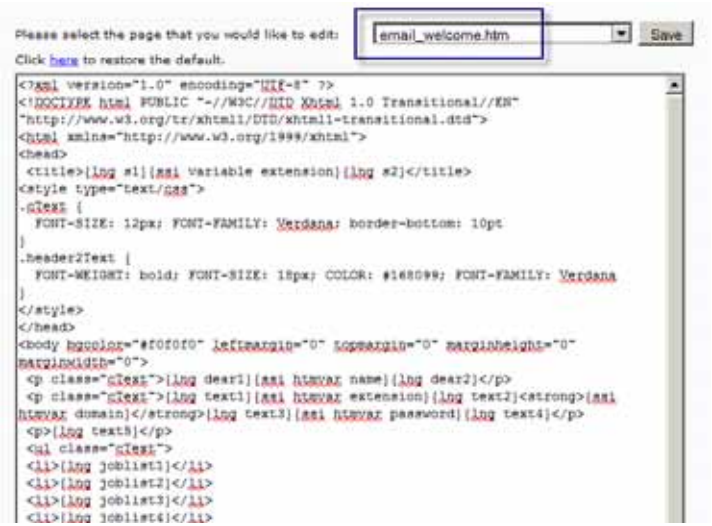
Templates

This page allows you to change the look and feel of the PBX web pages. It also allows you to change the various email templates, phone configuration templates, style sheets, etc.


Settings
Domains
Email
Web Page Control
Status
Templates
Translation
User Page Control
HTML Templates:
This page lets you change the look and feel of the PBX web pages. It also allows you to change the various email templates, phone config templates, style sheets, etc.
Please select the page that you would like to edit:
Please select page
Save
Click here to restore the default.
Please select page
aastra.txt
aastra_mac.txt
call_list_scripts.js
client_side_scripts.js
codec_selection.js
dialplan_test_script.js
dialplans.xml
dom_acclist.htm
dom_account_search.htm
dom_accounts.htm
dom_acd.htm
dom_acd2.htm
dom_acd3.htm
dom_acd4.htm
dom_acd5.htm
dom_acds_list.htm
dom_adrbook.htm
dom_adrbook_edit.htm
dom_att.htm

To customize the templates, a familiarity with HTML is required.

1. Navigate to **Admin** > **Web Page Control** > **Templates.**
2. From the dropdown, make a selection. The HTML will be displayed:



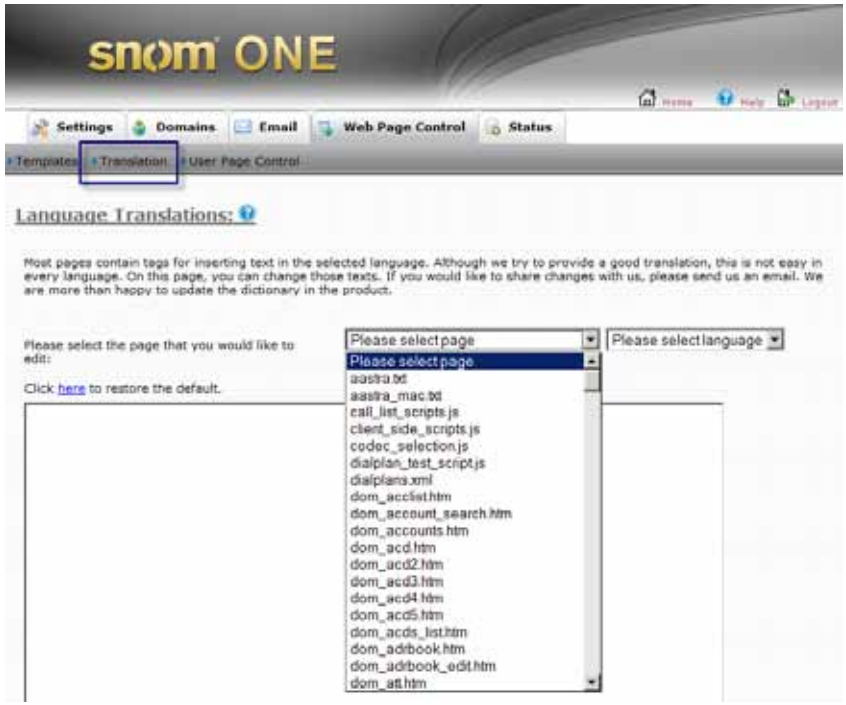
Embedded between the standard HTML tags (e.g., `<title></title>` and `<body></body>`) is additional code (`ssi htmvar password, lng text4, ssi var link`, etc.) that is used by the system to translate various parts of the welcome message, e.g., the specific extension that has been created, the language that has been set for that extension, etc. If these settings are not important and you prefer to send a static email once an extension has been created, you can create a static message similar to the following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//
EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.
dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>This email is sent by snom ONE</title>
<style type="text/css">
.normalText {
FONT-SIZE: 12px; FONT-FAMILY: Verdana; border-bottom: 10pt
}
```

```
.header2Text {
FONT-WEIGHT: bold; FONT-SIZE: 18px; COLOR: #168099; FONT-
FAMILY: Verdana
}
</style>
</head>
<body bgcolor="#f0f0f0" leftmargin="0" topmargin="0" margin-
height="0" marginwidth="0">
<p class="normalText">Hello new user. You have been added to
the snom ONE telephone system. This email is sent automati-
cally. Do not reply.
</p>
</body>
</html>
```

Translation

Although we try to provide good translations, it's not an easy task for every language. On this page, you can modify the text for the language you are using.



User Page Control

The **User Page Control** tab allows the administrator to control which fields are displayed on the user pages. Figure 2-4 shows the general settings that can be hidden from the user. These settings are detailed on the next page.

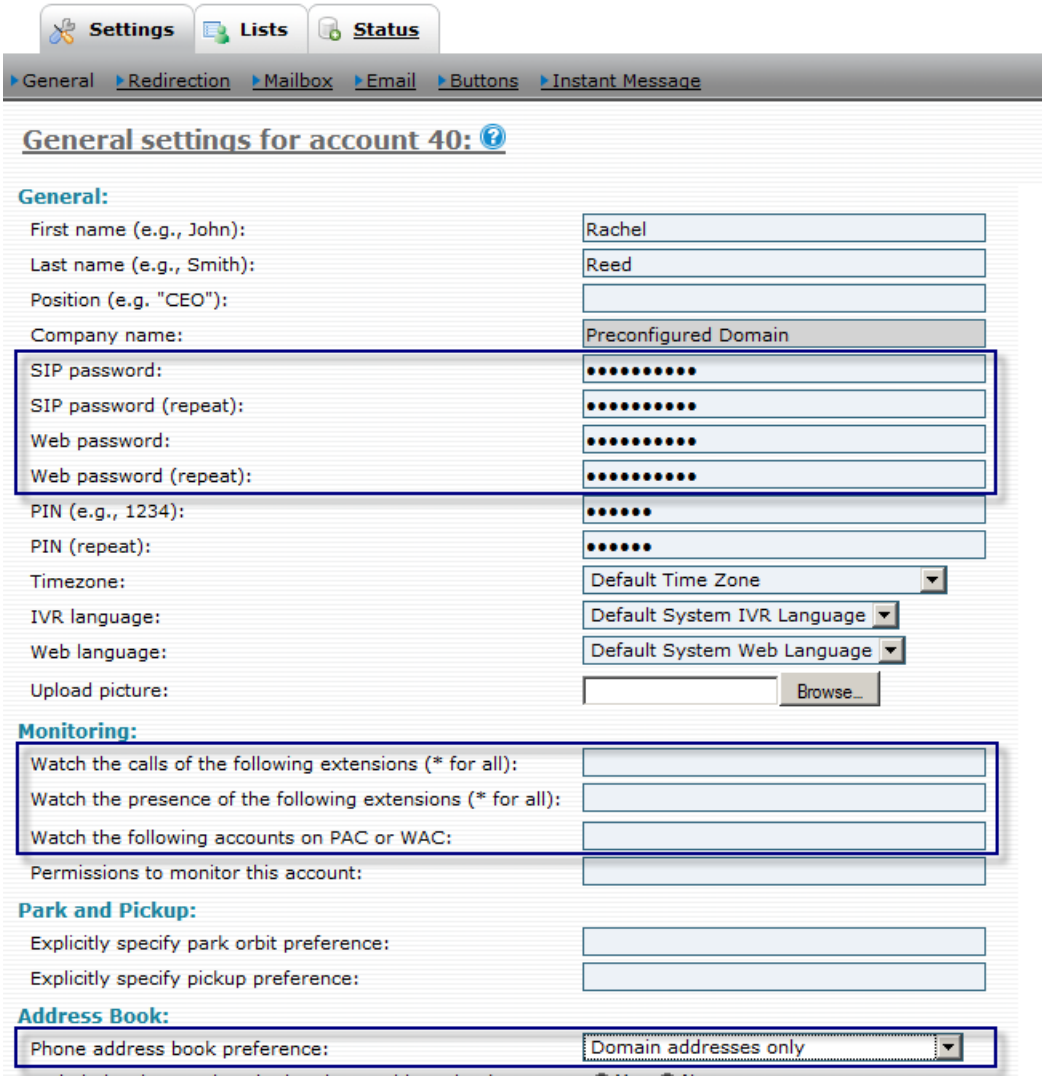


Figure 2-4. Blockable User Settings (**Settings** > **General**)

General Control

The General Control settings allow you to prevent the user from viewing the password fields and certain monitoring settings.

- **SIP password**: By preventing the user from seeing the **SIP Password** setting, the administrator can ensure that users will be unable to change their SIP passwords. This can save the administrator time spent in dealing with registration problems that result from changed SIP passwords.
- **Web password**: By preventing the user from seeing the **Web password** setting, the administrator can ensure that users will be unable to change their web passwords. This will prevent the user from forgetting a changed password and the administrator from having to issue a new one.
- **Calls, presence, PAC watch field:** This setting impacts the following user settings:
  - **Watch the calls of the following extensions**: This setting allows users to monitor the status of other extensions. Some users will need this setting (e.g., a boss who is monitoring certain employees, a secretary who needs to monitor the boss's extension, etc.). Other users, such as those working in a call center, will not need to monitor other people's extensions.
  - **Watch the presence of the following extensions**: This setting allows you to see a person's presence status (e.g., away, busy, DND) from the WAC and from some phones.
  - **Watch the following accounts on PAC**: This setting allows users to monitor extensions on the WAC. Not all users will need access at this level.
- **Phone address book preference**: This setting is applicable to the address book of the snom phone. It allows the user to upload the address book from the system to the snom phone directory.

Redirection Control

The Redirection Control settings allow you to prevent the user from viewing certain redirection settings. Figure 2-5 highlights these settings (details are provided below the image).

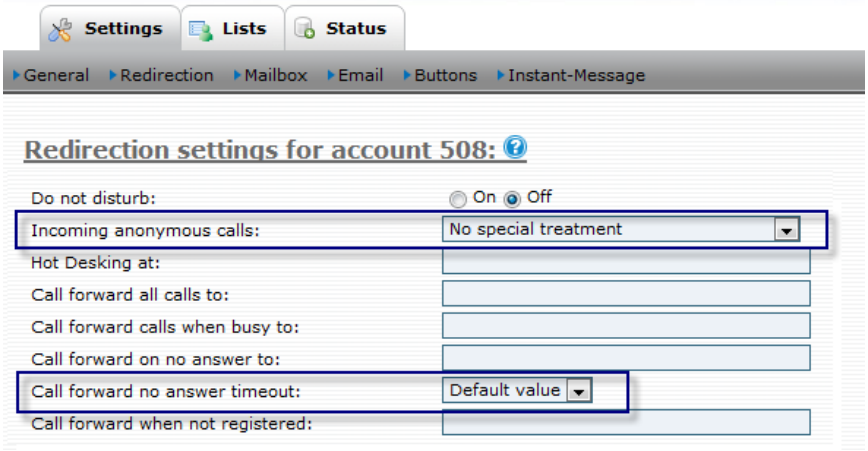


Figure 2-5. Blockable User Settings (**Settings** > **Redirection**)

- **Incoming anonymous calls**: This setting allows users to control the treatment of anonymous callers (reject them, pretend to be busy, ask for name, etc.). In some situations, administrators may prefer to determine how anonymous callers are handled.
- **Call forward on no answer timeout**: This setting allows users to specify the number of seconds that should lapse before the call is directed to voicemail. In situations where voicemail is not used, such as call centers, this setting is not necessary.

Mailbox Control

The Mailbox Control settings allow you to prevent the user from viewing various voicemail settings. Figure 2-6 highlights these settings (details are provided below the image).

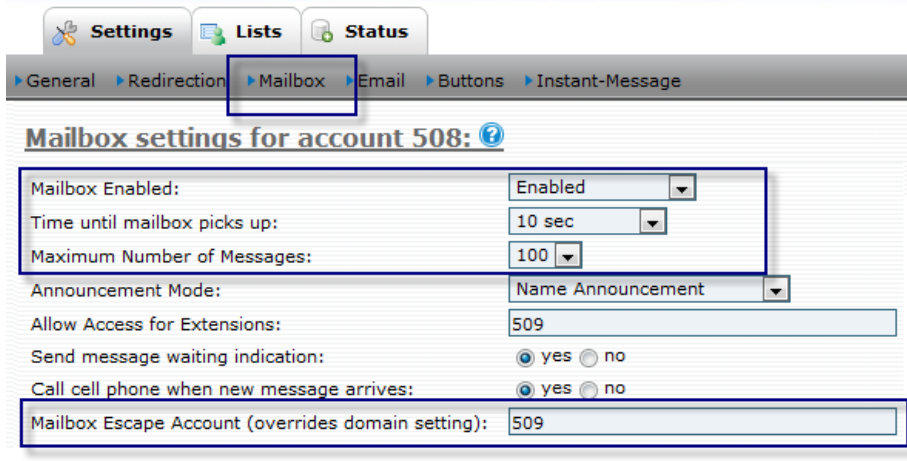


Figure 2-6. Blockable User Settings (**Settings** > **Mailbox**)

- **Mailbox enabled field**: This setting allows users to enable their voicemail. In situations where voicemail is not used, such as call centers, this setting is not needed.
- **Time until mailbox picks up**: This setting allows users to set their own mailbox pickup time and to allow their phone to ring for longer periods of time before it goes to voicemail.
- **Maximum number of messages**: This setting allows users to set the number of message that will be saved in their mailboxes. If space is an issue, administrators may want to place their own limit on this setting and prevent the user from changing it.
- **Mailbox escape account**: This setting gives users the option to change the direction of a call once the caller presses 0 to speak with the operator (calls are redirected to the escape account). In many cases, users will not have the option of directing their calls to another extension and will not need this setting.

Email Control

The Email Control settings allow you to prevent the user from viewing various email settings. Figure 2-7 highlights these settings (details are provided below the image).

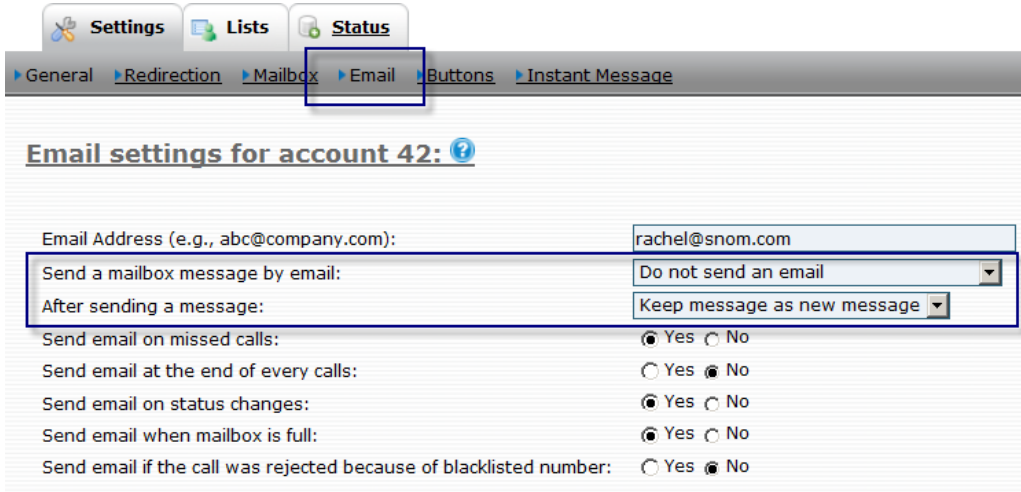


Figure 2-7. Blockable User Settings (**Settings** > **Email**)

- **Send a mailbox message by email**: This setting allows users to send voicemail messages to their email accounts. In situations where voicemail is not used, such as in call centers, this setting is not needed.
- **After sending a message**: This setting allows users to specify how messages that have already been read should appear (marked as new/read or deleted).

Chapter 3

ADMINISTERING THE DOMAIN

The snom ONE telephone system has multi-tenant capability (available in snom ONE blue[1] only). To implement this functionality, snom ONE uses domains. A domain can be thought of as a logical group of users and is very similar to email domains.

Email Domains	
User	Host
jack	google.com
jpiccolo	yahoo.com
rnti	aol.com

snom ONE Domains
pbx.companya.com
pbx.companyb.com
pbx.mycompany.pbx.com

Users within the same domain on snom ONE can call each other without going through a trunk. They can also access the same address book and share features, such as call monitoring and call park/pickup.

A snom ONE domain name should be fully qualified and configured in the DNS server so that traffic can be routed to the proper IP address of the PBX. If this is not possible, then you can set the outbound proxy field in the system. This will configure the registrar to the domain name. If you have only one domain on the system, be sure to leave the alias `local host` as the domain name or as the alias to it. This will enable snom ONE to locate extensions without looking at the domain name.

1. snom ONE blue supports multi-tenant use for up to five companies. Multi-tenant use is not available for snom ONE yellow and snom ONE free.

Naming the Domain

By default, the system installation creates `pbx.company.com` and associates `localhost` as alias to it.

Default Domain	Alias
`pbx.company.com`	`localhost`

The `localhost` domain will match all requests that cannot be matched to a domain name within the domain list. This makes it possible to run the system on changing IP addresses without changing the name of the domain.

You may use several names for a domain; this is known as domain aliases. However, one of the names will be the primary (canonical) name for the domain. The system will use that name whenever it has to generate a name for the domain.

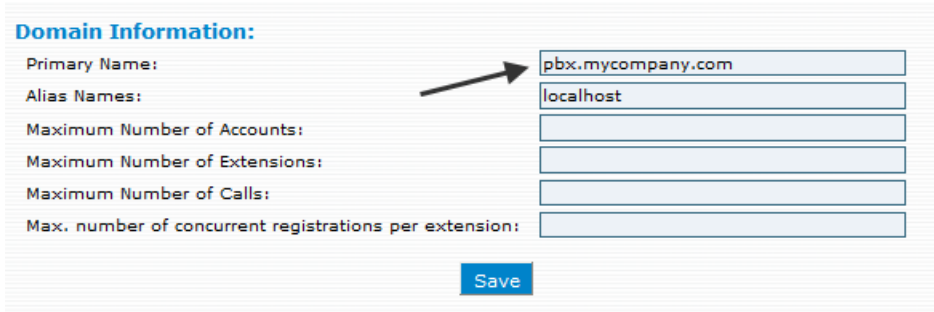
Domain names may also be IPv4 addresses when you cannot change the DNS. However, if you are assigning IP addresses by DHCP, be careful with this method. Make sure that the host is always running on that IP address. You may mix IPv4 names with DNS addresses, and you may also later rename the domain names and reassign the primary domain name.

Changing the Name of the Domain

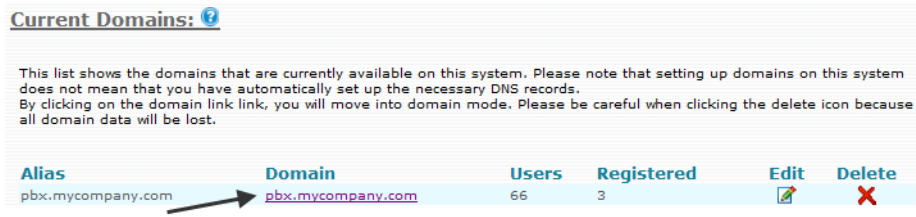
To change the name of the default domain so that it reflects your company domain:

1. Navigate to **Domains** and click the **Edit** icon.

2. Replace `pbx.company.com` with your own domain name.



3. Enter an alias if desired.
4. Click **Save**.
5. Click **List** to view the domain. The new domain will be displayed.


Current Domains:
This list shows the domains that are currently available on this system. Please note that setting up domains on this system does not mean that you have automatically set up the necessary DNS records.
By clicking on the domain link link, you will move into domain mode. Please be careful when clicking the delete icon because all domain data will be lost.
Alias
Domain
Users
Registered
Edit
Delete
pbx.mycompany.com
pbx.mycompany.com
66
3

Note: Setting up a domain on the system does not imply that the necessary DNS records have automatically been set up. If you can, set up your DNS so that users from other domains can find the group by standard DNS name resolution (e.g., `pbx.company.com` = `75.1.2.4`, the IP address of the system).

Assigning a Domain Administrator

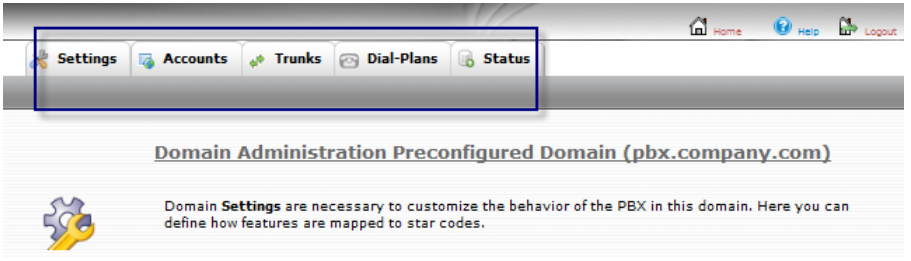
Just as the system is managed, so must the domain be. This can be the role of the administrator or a user who is assigned by the administrator (the administrator will always have access to both system and domain settings). Whether the administrator assigns someone or not is usually based on the size of the company and how much responsibility the administrator wants to delegate. The responsibilities of the domain administrator involve extension accounts, trunks, and dial plans, but the administrator can also limit many of these settings (see the **Allow domain admin . . .** settings on page 52).

The permission to manage the domain should be given only to those who are allowed to change passwords, create or delete accounts, change dial plans and rates, and so forth. Permission is given from the **Permission** tab in the user's extension account:

To log in to the domain, users will need to log in as Domain Administrator (with their extension credentials) as shown below:

Please enter your login information. In environments with multiple domains, you have to use an account name like "username@domain". In environments with only one domain, you can use the form "user". For more information about the login procedure, please see the online documentation.
PBX Login
Account:
51
Password:
Login Type:
Automatic
Language:
Automatic
User Login
Domain Administrator
System Administrator
Console Login

Once logged in, domain administrators will be able to access the domain settings shown below.



The settings associated with the domain tabs are briefly outlined in Figure 3-1 and are described in more detail in Table 3-1.

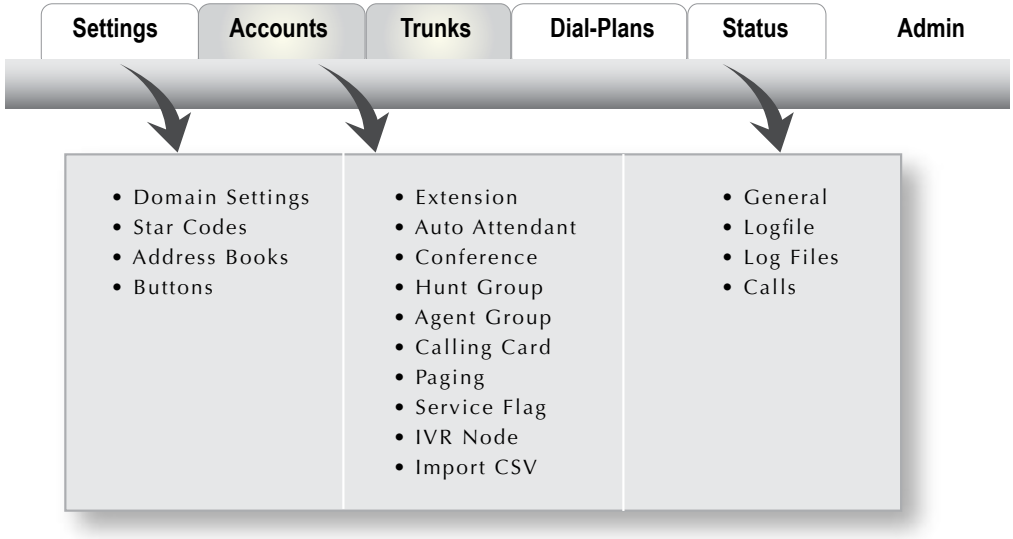


Figure 3-1. Outline of Domain Web Interface

Table 3-1. Menu Tree of Domain Tabs

Web Interface Tab	Description
Settings	
Domain Settings	This page allows you to configure the necessary settings for the domain. From this page, you can decide which dial plan, language, and music on hold source the domain will use. You can also enable features such as camp-on, trust caller-ID, and voicemail timeout.
Star Codes	This page lists the star codes that are used to control the system. From this page, you may define your own set of star codes.
Address Book	This page lists all the names and contact information of those who are part of the domain. From this page, you can add individual entries to the address book, or you can upload a CSV file to add a large number of names.

Web Interface Tab	Description
Buttons	This page provides a list of all the button profiles that are available on the domain. From this page, you can create additional button profiles.
Accounts	This tab provides a listing of the accounts that have been created on the domain. This includes extensions, hunt groups, agent groups, service flags, paging accounts, and any other account that exists on the domain. Accounts can be created, edited, and deleted from this page.
Trunks	This tab provides a listing of the trunks that have been created on the domain. New trunks can be created at this page, and existing trunks can be edited and deleted.
Dial Plans	This tab provides a listing of all the dial plans that have been created on the domain. New dial plans can be created at this page, and existing dial plans can be edited and deleted.
Status	
General	This page shows you a snapshot of your system: release of software, type of software, expiration date, etc.
Logfile	This page displays the SIP messages, which can be used for troubleshooting.
Call Log	This page displays a list of calls that have been made through the system.
Calls	A list of active calls are displayed on this page.

Domains—Default and New

Default Domain

The system comes with a preconfigured domain that includes ten 2-digit extensions and numerous domain accounts (Figure 3-1). To view the accounts, click **Accounts** > **List**.

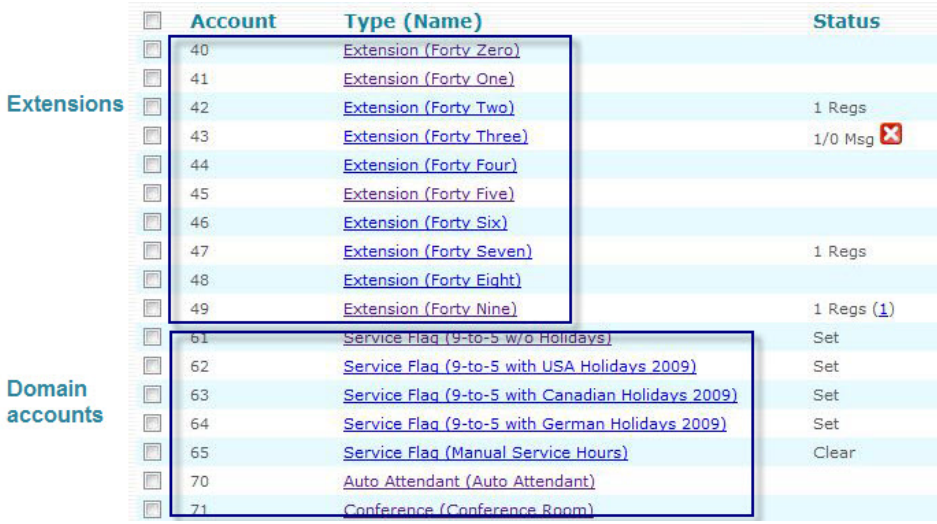
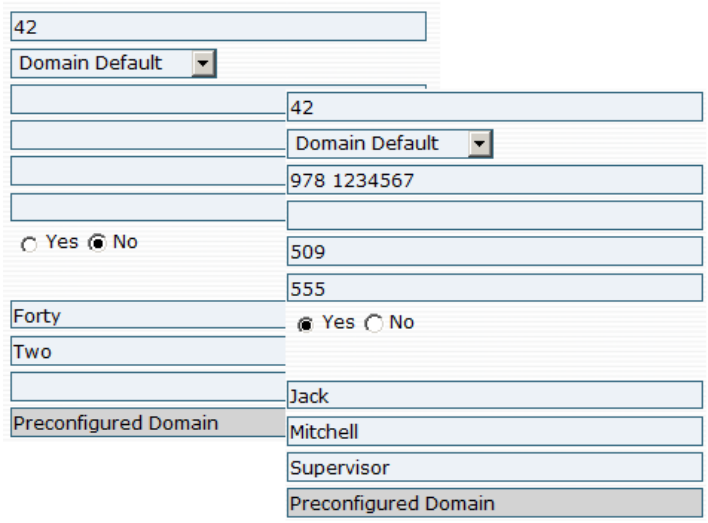

Account
Type (Name)
Status
Extensions
Domain accounts
40 Extension (Forty Zero)
41 Extension (Forty One)
42 Extension (Forty Two) 1 Regs
43 Extension (Forty Three) 1/0 Msg
44 Extension (Forty Four)
45 Extension (Forty Five)
46 Extension (Forty Six)
47 Extension (Forty Seven) 1 Regs
48 Extension (Forty Eight)
49 Extension (Forty Nine) 1 Regs (1)
61 Service Flag (9-to-5 w/o Holidays) Set
62 Service Flag (9-to-5 with USA Holidays 2009) Set
63 Service Flag (9-to-5 with Canadian Holidays 2009) Set
64 Service Flag (9-to-5 with German Holidays 2009) Set
65 Service Flag (Manual Service Hours) Clear
70 Auto Attendant (Auto Attendant)
71 Conference (Conference Room)

Figure 3-1. Default Accounts

Note: A yellow triangle symbol indicates that the account is missing either the SIP password or the web password.

Modifying the Default Domain

To modify the accounts in the default domain, click the account and replace the existing information with new information.

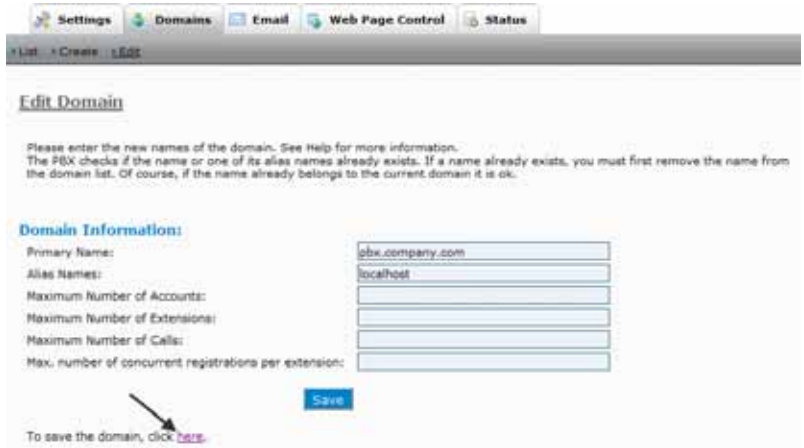


Creating New Domains

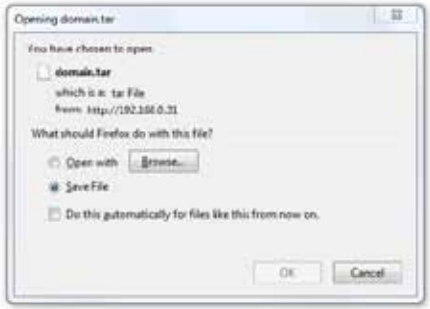
When creating new domains, copying an existing domain is the simplest method. To do this, you will need to create a tar file; tar files are commonly used to collect many files into one larger file, while preserving file system information. With snom ONE, information such as account information, trunks, dial plans, and system settings will be retained. To create a tar file:

1. Navigate to **Domains**.
2. Click **Edit** for the domain you would like to use as a template.

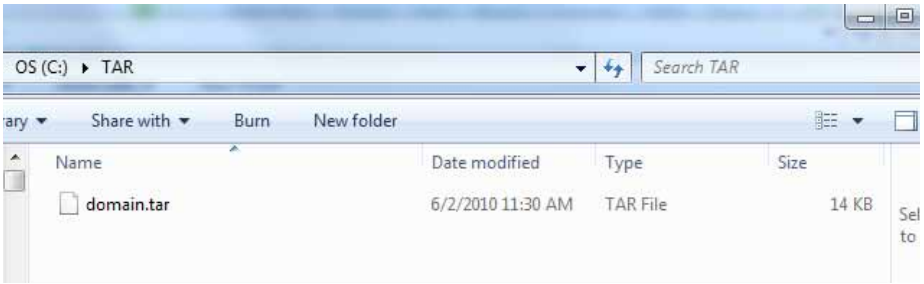
3. Click the link at the bottom of the page to save the domain.


Settings
Domains
Email
Web Page Control
Status
List
Create
Edit
Edit Domain
Please enter the new names of the domain. See Help for more information.
The PBX checks if the name or one of its alias names already exists. If a name already exists, you must first remove the name from the domain list. Of course, if the name already belongs to the current domain it is ok.
Domain Information:
Primary Name:
pbx.company.com
Alias Names:
localhost
Maximum Number of Accounts:
Maximum Number of Extensions:
Maximum Number of Calls:
Max. number of concurrent registrations per extension:
Save
To save the domain, click here.

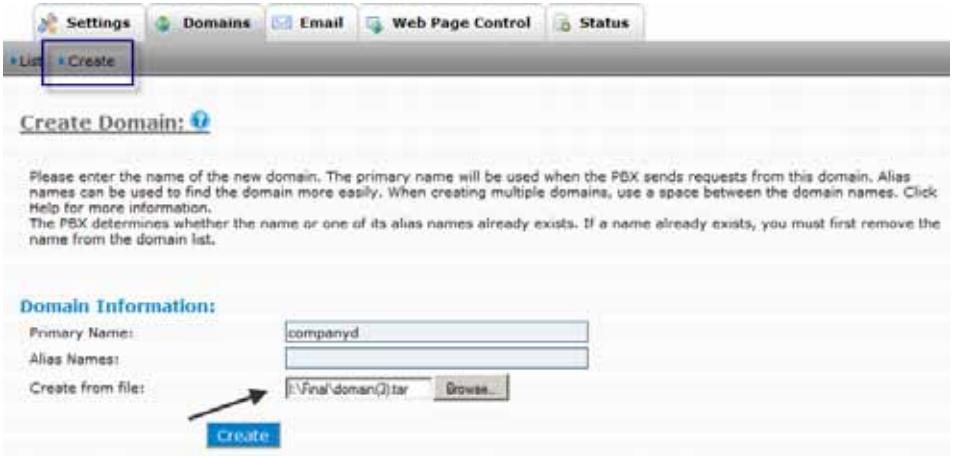
4. Click **Save File**.



5. Browse to the location where the file will be saved:



6. Click **Create** as shown below:


Settings
Domains
Email
Web Page Control
Status
List
Create
Create Domain:
Please enter the name of the new domain. The primary name will be used when the PBX sends requests from this domain. Alias names can be used to find the domain more easily. When creating multiple domains, use a space between the domain names. Click Help for more information.
The PBX determines whether the name or one of its alias names already exists. If a name already exists, you must first remove the name from the domain list.
Domain Information:
Primary Name:
companyd
Alias Names:
Create from file:
Browse...
Create

7. Using the **Primary Name** field, name the domain.
8. Click **Browse** (shown above) and navigate to the tar file.
9. Click **Create**.
10. Once the page has finished loading, click **List**. The new domain will be listed:

11. To set up the domain, click the domain and add the accounts from there.

Configuring the Domain

From the **Settings** tab, you can configure many domain settings:

- **Name of the Domain:** This field allows you to give the domain a descriptive name. The name can contain special characters and spaces and may include upper and lowercase characters. The name will be used by the system when sending emails with call data records for the domain. This name is independent from the domain name that is set by the system administrator.
- **Default Dial Plan:** This dial plan will be used by the domain, but users can override this with their own dial plan based on need. Most of the accounts in a domain will use the default dial plan. If you do not set a default dial plan, you will likely have problems placing outbound calls. Therefore, it is strongly recommended to choose a default dial plan.
- **Default IVR Language:** This setting can be configured by the administrator and is not needed on the domain level in single-domain environments.
- **Tone Language:** This setting can be configured by the administrator and is not needed on the domain level in single-domain environments.
- **Default Web Language:** This setting can be configured by the administrator and is not needed on the domain level in single-domain environments.
- **Music on Hold Source:** You can select the source of music that will be used when a call is put on hold. The party who is on hold hears the music that is chosen here. See also Chapter 21, "Music on Hold."
- **Timezone:** The system can handle multiple time zones simultaneously, making it possible for users to select a time zone that corresponds with their geographic location. This setting influences the time on mailbox messages and the telephone display. Before the system can apply the time zone to the user's extension, it needs a time zone configuration file (`timezones.xml`), which is encoded in XML and looks similar to the following:

```
<?xml version="1.0" encoding="utf-8"?>
<timezones dict="timezones.xml">
 <zone name="AKDT">
  <description>Alaska Time Zone</description>
  <gmt_offset>-32400</gmt_offset>
  <dst_offset>3600</dst_offset>
  <dst_start_day_of_week>1</dst_start_day_of_week>
  <dst_start_month>4</dst_start_month>
```

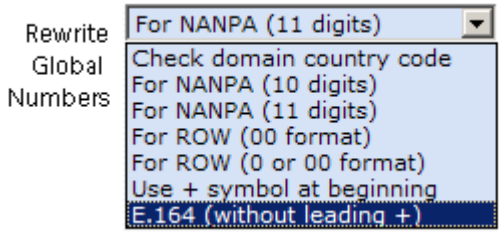
The name of the time zones is reflected in the `lang_xx.xml` file, where xx is replaced by the respective language (see Table 18-5 for a list of language code identifiers).

- **Country Code:** The country code plays a major role in interpreting telephone numbers. Three modes are available for this setting.

Table 3-2. System's Interpretation of Telephone Numbers

Modes	Description	Input
As Is	If this setting is left empty, the system does not change telephone numbers. In this case, you must make sure that users, PSTN gateways, and service providers use the same method of representing a number (for example, 10 or 11 digits in the United States). Choose this mode when the other modes are causing problems.	Leave empty
NANPA	If you enter a `1` into the Country Code field, the system will interpret telephone numbers according to the NANPA scheme (North American Numbering Plan Administration), which means that international numbers will start with 011 and numbers that have 10 digits will be written in the (xxx)xxx-xxxx scheme (JavaScript takes care of this in the web interface). This scheme also applies to countries other than the United States, like Canada. Apart from the readability of numbers, this scheme has the added benefit of automatically converting differently represented numbers (11-digit or 10-digit) into a global format. The area code must be 3 digits and is used for numbers that have only 7 digits.	`1`
ROW	If you enter another country code into this field (for example, `33` for France), the system will interpret numbers according to a "rest of world" scheme, which means that international numbers start with 00 and national numbers start with 0. The area code is used to determine whether the short number format can be used or not (local call).	Any country code (e.g., `33`)

The **Country Code** setting corresponds to the **Rewrite global numbers** setting (page 140):


Rewrite Global Numbers
For NANPA (11 digits)
Check domain country code
For NANPA (10 digits)
For NANPA (11 digits)
For ROW (00 format)
For ROW (0 or 00 format)
Use + symbol at beginning
E.164 (without leading +)

- **Area Code:** This is the telephone area code for the domain. This is generally NPA in the NPA-NXX-XXXX number (e.g., `978`, `212`, etc.).
- **Default ANI:** Using this setting, you can configure each domain with a default ANI (Automatic Number Identification). ANI is a service that tells the recipient of a telephone call which telephone number made the call. In most cases, the ANI is used in the `From` field in the SIP packets or the caller-ID.

- **Trust Caller-ID:** This setting is used to specify whether the caller-ID should be used to authenticate, rather than asking users to enter their PIN numbers.
- **Emergency Numbers:** You can specify special destination numbers when an extension dials an emergency number. The number(s) that trigger the mechanism must be listed in this setting. If you have more than one emergency number, use a space between the numbers (e.g., `911 199`). By default, this setting is blank (i.e., it is not set to 911).
- **Use last 7 digits when cellphone matching**: If this is checked, the system will use the last 7 digits to match cell phone numbers. This is useful in places where only 7 digits are used in the caller-ID.
- **Send welcome email when an extension is created:** If this setting is checked, new users will automatically receive a welcome email.

- **Delete all aliases when deleting the primary account:** Aliases will be deleted when primary accounts are deleted.

From/To Headers

- **From header when switching the domain:** This setting allows you to set a new `From` header. It is used when the system switches the domain context for calling an extension. You may enter several dollar-escaped characters into this field using the values shown in Table 3-3. For example, the string `$d: $n` will produce an output like **`Company A: John Smith`** if the source domain name was set to `Company A` and the original content of the header was `John Smith`. If this setting is empty, the system will not change the header.

Table 3-3. Parameters Used for Setting the From and To Header

Value	Output	Example
`d`	The domain name of the calling (source) domain	`Company A`
`e`	The domain name of the called (destination) domain	`called.domain.com`
`n`	The original content of the header	`John Smith`
`x`	Parameter 1 of the called extension	
`y`	Parameter 2 of the called extension	
`z`	Parameter 3 of the called extension	

`x`, `y`, and `z` are fields that can be used for additional information.

- **To header when switching the domain:** This setting allows you to set a new `To` header. It is used when the system switches the domain context for calling an extension. You may enter several dollar-escaped characters into this field using the values shown in Table 3-3.
- **Change names in To/From-headers:** Usually it is okay if the system changes the names in the `To/From` headers in the SIP packets. For example, this makes sense when the address book matches the caller-ID and the system should present the address book entry. However, if the system is used as a SIP

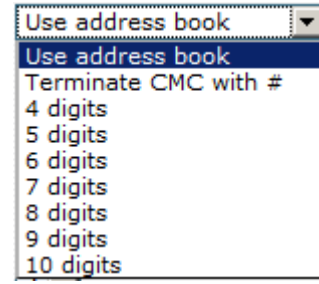
device in an operator environment, you may want to make sure that the system does not change headers. In such cases, this setting should be set to **Yes**.

CDR Settings

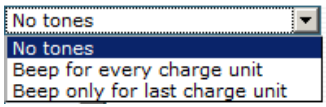
- **CDR URL**: This setting allows you to configure where and how the CDRs are written for a specific domain. This setting will override the configurations that are made at the system level for the domain. The system supports several types of CDR generation formats, apart from writing them into the `<pbx install dir>/cdr` directory in XML format (see the **CDR URL** setting on page 47).

Billing Settings

- **CMC authentication for outbound calls:** This setting works in tandem with the "C" checkbox in the dial plan (page 148). When the "C" is checked, this domain setting will be used; otherwise, it will be ignored. This setting dictates at what point, after a CMC code has been entered into the phone, the system will begin looking for a match. When **Use address book** is selected, the system will automatically take the CMC from the address book record.



- **Billing Tones:** This field allows you to configure whether domain users will hear a beep during the call when using the pre-pay feature of the system (pre-pay is discussed in Chapter 16).



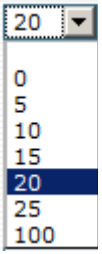
- **Credit for outbound calls:** This setting allows you to place a limit on outbound calling for the entire domain. Once the extensions as a group have reached the maximum, outbound calls can no longer be placed. This setting can also be configured at the extension level (see **Credit for outbound calls** in page 171).

Voicemail/Mailbox Settings

- **Time until user's mailbox picks up:** This setting defines the number of seconds the system will wait before redirecting a call to a user's mailbox when there's been no pickup. You may override this setting in the settings for a specific extension. If you plan to use cell phones with the system, choose a longer voicemail timeout (e.g., 30 seconds), as the call setup time for a cell phone call can be lengthy and the user might need to search for the cell phone. If you do not plan to use cell phones, you can choose a shorter timeout (e.g., 15 or 20 seconds).

These next two settings allow you to specify memory capacity for voicemail messages. When configuring these settings, consider the size of your system and the information shown in Table 3-4.

- **Voicemail Size:** This setting determines the number of messages that can be stored in a user's voicemail box. Although this setting can be overridden by the user (see the **Maximum number of messages** setting on page 413), a reasonable default should be set at the domain level (`20` is a good default number). If this setting is left blank, the number of messages that can be stored in a user's mailbox will be unlimited.



- **Maximum Voicemail Duration:** This setting specifies the length of a mailbox message. Typically, a mailbox message should be no longer than 2 minutes. If this setting is left blank, the length of any one message can be unlimited.

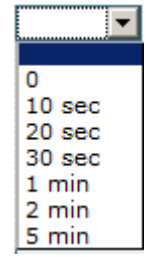
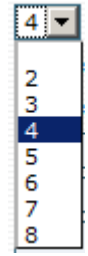


Table 3-4. Voicemail and Disk Space Requirements

Number of Users	Settings		Disk Space Required*	
	Voicemail Size	Voicemail Duration	Each User	All Users
10	25	2 minutes	5 MB	50 MB
10	100	2 minutes	20 MB	200 MB
100	25	2 minutes	5 MB	5 GB
100	100	2 minutes	20 MB	20 GB

*1 minute of voicemail or call recording requires approximately 100 kb of disk space. Based on this measurement, you can record 165 hours of voicemail per gigabyte.

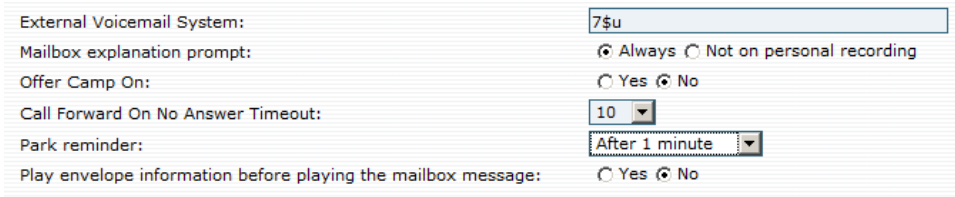
- **Voicemail PIN Digits:** This setting specifies the number of digits that will be required for the voicemail PIN. Although any number larger than one digit is acceptable, we recommend you require four or five digits. See also the **PIN** setting in the extension account (page 166).



- **Require Entering Mailbox PIN:** When this setting is enabled, users will be required to enter their PIN before retrieving voicemail messages. While retrieving messages should be simple, many office layouts often make it too easy for an unauthorized person to listen to another's voicemail messages without authorization. This setting can be used to prevent this across the domain.

- **Calling own extension number goes to mailbox:** By default, the system will send a user to the voice mailbox if he dials his own extension. However, in some situations it is useful to have the system call the registered extension.
- **Mailbox Escape Account:** If the Mailbox Escape Account setting is set, a user who reaches the mailbox can press 0 to get to the account that you specify here (the user must press 0 before the beep). The number must be an internal number.
- **Mailbox Direct Dial Prefix:** This setting allows users to call directly into their mailboxes or transfer a caller directly to a user's voicemail without having to wait for the voicemail timeout. Typically, this prefix is an `8`, so by dialing `8511`, the caller goes directly to the voicemail greeting of extension 511.

- **External Voicemail System:** This setting is used if you want to use an external voicemail system (e.g., Microsoft Exchange 2007/2010). The setting requires a telephone number that can be dialed and can include replacement fields which are used in the caller-ID representation for outbound calls. The dial plan for the called extension will decide which trunk will be used to send the call. See Appendix C for more information on Exchange.
- **Mailbox Explanation Prompt:** Users who configure their extension to play a personalized message when callers reach their extension can activate this setting so that the system will deliver an explanatory message after the playback of the personalized recording. The explanatory message explains that the caller may now leave a message and informs the caller of any other options. For standard greetings, the system always explains the options.
- **Offer Camp On:** This setting allows you to offer Camp On to callers, rather than limiting them to leaving voicemail. Callers will have the option to press 1 for a callback. Turn this off if you are using external voicemail systems such as Microsoft Exchange.

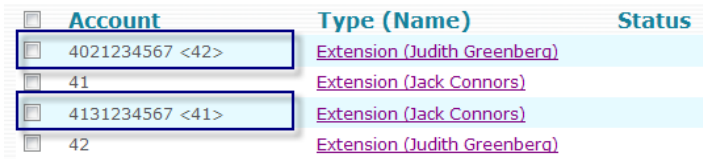


- **Call forward on no answer timeout:** This setting establishes the number of seconds that the system will wait before performing a timeout action. It is advisable that this setting be less than the voicemail timeout; otherwise, the call will not be forwarded and will instead go to voicemail.
- **Park Reminder:** When this setting is enabled, the system will call back an extension that has parked a call, as a reminder that a call is still parked. Specify the amount of time that should pass before the reminder is made.
- **Play envelope information before playing the mailbox message**: When this setting is enabled, envelop information will be offered to the user while retrieving voicemail messages. To retrieve the information, the user can press #5. (If this setting is not turned on and the user presses 0 to hear more options, the envelop information will be offered at that point.)

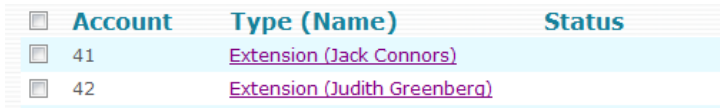
Accounts Page Display

- **Accounts page size**: This setting determines how many accounts appear on one page. The options range from 25–1000 accounts (all accounts can be viewed if desired).
- **Hide aliased accounts under accounts page:** This setting allows you to hide all alias accounts. (Aliases are DID numbers and are used for direct dialing.) When this setting is set to **Yes**, aliased accounts will not be displayed:

Before (set to No):

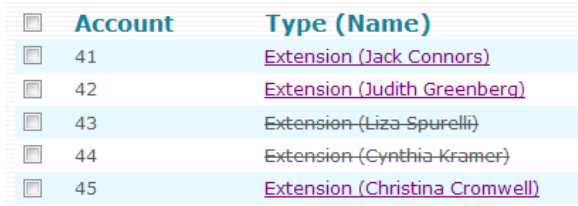


After (set to Yes):

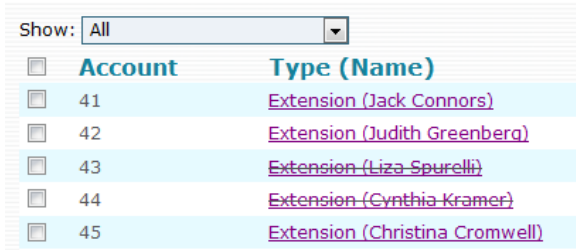


- **Display hyperlink for the disabled accounts in the accounts page**: When this setting is set to **Yes**, disabled accounts will be hyperlinked to the actual account:

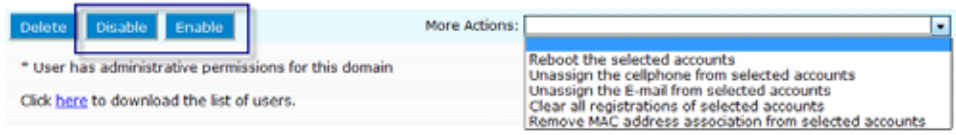
Before (set to No):



After (set to Yes):



Accounts can be disabled and enabled using the **Disable** and **Enable** buttons at the bottom of the **Accounts** page. Additional actions are shown in the dropdown.


Delete
Disable
Enable
More Actions:
* User has administrative permissions for this domain
Click here to download the list of users.
Reboot the selected accounts
Unassign the cellphone from selected accounts
Unassign the E-mail from selected accounts
Clear all registrations of selected accounts
Remove MAC address association from selected accounts

- **Display MAC address for the accounts in the accounts page:** When this setting is activated, the MAC address for each account (if one is available) will be displayed. When the permanent or temporary assignment mode is used for

obtaining MAC addresses, a question mark or asterisk will appear in the MAC address field.

Account	Type (Name)	Status	MAC Address
41	Extension (Jack Connors)		01:23:45:67:89:ab
42	Extension (Judith Greenberg)		01:23:45:67:89:ac
43	Extension (Liza Spurelli)		01:23:45:67:89:ad
44	Extension (Cynthia Kramer)		01:23:45:67:89:ae
45	Extension (Christina Cromwell)		*

- **Display Email address for the account in the accounts page:** When this setting is activated, the email address for each account (if one is available) will be displayed:

Account	Type (Name)	Status	Email
41	Extension (Jack Connors)		connors@company.com
42	Extension (Judith Greenberg)		judith@company.com
43	Extension (Liza Spurelli)		liza@company.com
44	Extension (Cynthia Kramer)		cynthia@company.com
45	Extension (Christina Cromwell)		christina@company.com

- **Display cell phone for the account in the accounts page:** When this setting is activated, cell phone numbers that have been configured to an account will be displayed:

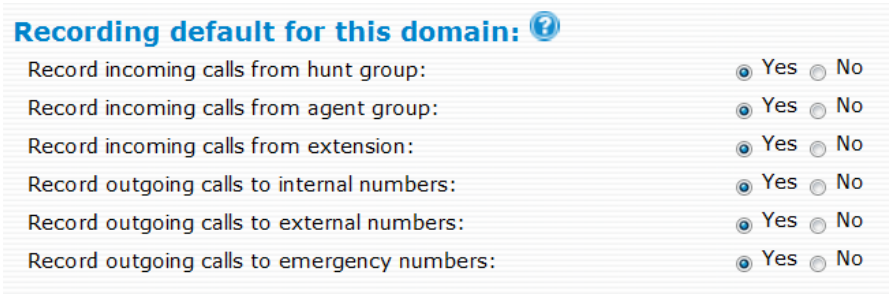
Account	Type (Name)	Status	Cell Phone
41	Extension (Jack Connors)		9871234567
42	Extension (Judith Greenberg)		
43	Extension (Liza Spurelli)		
44	Extension (Cynthia Kramer)		978345123x
45	Extension (Christina Cromwell)		6031234567

All three fields can be displayed at the same time:

Account	Type (Name)	Status	MAC Address	Cell Phone	Email
41	Extension (Jack Connors)		*	9871234567	connors@company.com
42	Extension (Judith Greenberg)		*		judith@company.com
43	Extension (Liza Spurelli)		*		liza@company.com
44	Extension (Cynthia Kramer)		*	978345123x	cynthia@company.com
45	Extension (Christina Cromwell)		*	6031234567	christina@company.com

Recording Defaults

This section allows you to define domain-level call recording settings. Recorded calls will be saved in the `recordings` directory (see also Chapter 18).

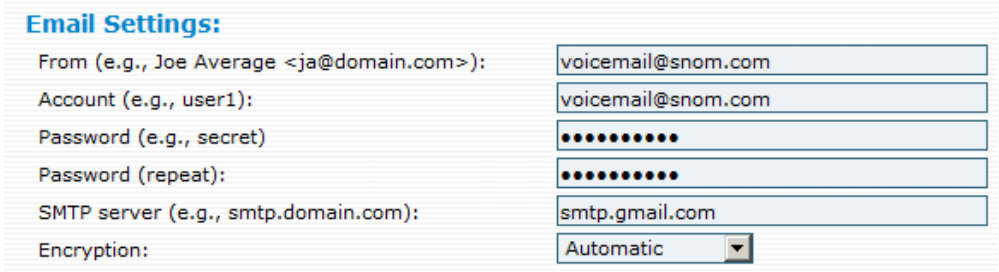

Recording default for this domain:
Record incoming calls from hunt group: Yes No
Record incoming calls from agent group: Yes No
Record incoming calls from extension: Yes No
Record outgoing calls to internal numbers: Yes No
Record outgoing calls to external numbers: Yes No
Record outgoing calls to emergency numbers: Yes No

- **Record incoming calls from hunt group:** This setting controls the recording on an extension (applies to calls coming from the hunt group for the entire domain).
- **Record incoming calls from agent group:** This setting controls the recording on an extension (applies to calls coming from the agent group for the entire domain).
- **Record incoming calls from extension:** This setting controls the recording on an extension (applies to calls coming from another extension for the entire domain).
- **Record outgoing calls to internal numbers:** This setting controls the recording on an extension (applies to calls going to another extension for the entire domain).
- **Record outgoing calls to external numbers:** This setting controls the recording on an extension (applies to calls going to external numbers for the entire domain).
- **Record outgoing calls to emergency numbers:** This setting controls the recording on an extension (applies to calls going to an emergency number).

Email Settings

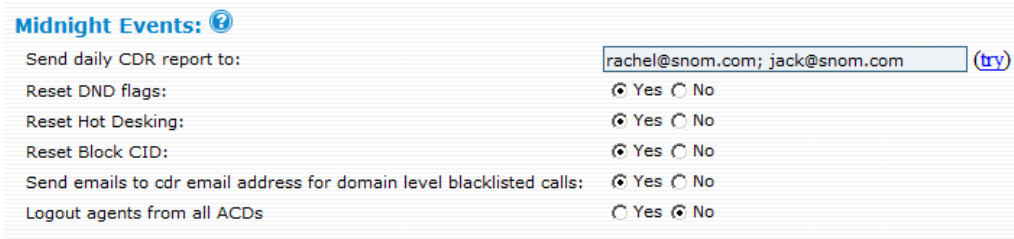
The system can be configured to send out emails on important occasions, but it needs an SMTP server to do this. From this page, you can configure the SMTP server settings

(these settings can also be made by the administrator by going to **Admin** > **Email)**. If the administrator has opted to use the same email settings across all domains, the email settings shown below will not be displayed at the domain level (see page 297).



Midnight Events

At midnight, the system can perform several maintenance tasks, including the generation and sending of CDR reports.



- **Send daily CDR report to:** The system sends daily CDR reports (sample shown in Figure 3-2) to the email addresses listed in this field. Use semicolons between multiple email addresses, since email addresses may contain spaces (e.g., `Fred Feuerstein <ff@domain.com>; Carl Clements <cc@domain.com>`). To test this feature, click the **Try** button once you've entered an email address rather than waiting until midnight. Keep in mind that this is just a link, and you may have to save your list before clicking the link. The report shows a running list of the previous day's calls:

From: voicemail@snom.com [mailto:voicemail@snom.com]
Sent: Thursday, October 29, 2009 12:00 AM
To: rachel@snom.com
Subject: Head Office: Calls on 2009/10/28

The following calls were made in the domain on 2009/10/28

Total number of calls: 154. Total duration: 9:22:26.

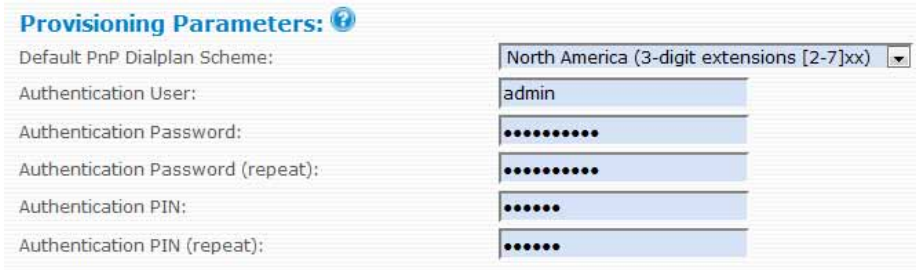
Time	From	To	Duration
2009/10/28 06:15:12	Jack Smith 9871234567	03031234567	00:02
2009/10/28 08:52:27	(604)1234567	(978)746-2777	00:03
2009/10/28 09:16:49	16621234567	19781234567	00:11
2009/10/28 09:16:25	1(662)862-8888	Stanley (506)	00:45

Figure 3-2. Sample CDR Report

- **Reset DND Flags:** DND is a major problem if users forget that they've set their extensions to DND and then open a trouble ticket next morning because they've stopped receiving calls! This setting can prevent that. When the **Reset DND Flags** has been enabled, the system resets all DND flags on the domain each day at midnight.
- **Reset Hot Desking:** Forgetting to deactivate a Hot Desking situation has similar consequences to forgetting to turn off DND, so use this setting if you want the system to reset hot desking each day at midnight.
- **Reset Block CID:** As with the previous two settings, this is another setting that is beneficial to reset each day at midnight.
- **Send emails to CDR email address for domain level blacklisted calls:** When someone calls into the auto attendant, hunt group, or agent group and is put onto the blacklist, the system will notify the person who receives the CDR report. The report will be sent daily at midnight.
- **Log out agents from all ACDs:** When this setting is enabled, all agents will be logged out of all agent groups each day at midnight.

Provisioning Parameters

When the system automatically generates files for the configuration of extensions, it needs a few settings from the domain.



- **Default PnP Dialplan Scheme:** This setting allows you to set auto-dial and configure timeout-based dialing. These settings are used by the phone and *not* the system (see Chapter 5 for the dial plan that is used by the system). The **PnP Dialplan Scheme** setting allows you to tell the system how many numbers your extensions contain (either 2, 3, or 4 digits). This will initiate automatic dialing once the required number of digits have been entered. If your extensions are all 3 digits long and include only digits 2 through 7, you should choose `3-digit extensions [2-7]xx`. Then if a user dials `201`, the system will identify that an extension has been dialed and will not wait for more digits. If NA is set and **Country Code** 1 is used, then anytime someone dials 1, the system will know to dial that country. For this reason, extensions should not begin with a 1.
  - User must press enter: When this scheme is selected, the user of the extension will be required to press the confirm button on the phone before the dialing will begin. This behavior is similar to cell phones, where users are required to press the green send button. This scheme can prevent problems because it is difficult to predict how many digits the phone must collect before it has enough digits for a complete number.
  - When the user is located in the North America area (www.nanpa.com), the length of the number is predictable for national calls and calls of other extensions in the domain. However, calls to international destinations or star codes are difficult to predict, so users will be required to press the confirm button to start the call.
  - For other countries, the "Europe" scheme might be appropriate. As with the rest of the world outside of NANPA, the length of a telephone number is practically unpredictable and users will be required to press

the confirm button to start the call. The "Europe" scheme will dial automatically only if the destination is another extension.

Note: If you want to create a customized dial plan, you can do this from either the snom phone or through the binary files of the system. In the case of the latter, you will need to request the appropriate file from snom and place it into the snom/`snomONE/html` directory (you may need to create the `html` directory). After you have modified the file, save it and reboot both the phone and the system.

Example: In the event you want to exclude numbers higher than 5 from the default of `[2-7]xx` so that users will not be required to enter a 1 when dialing local numbers beginning with 604 or 778, you need to replace `[2-7]` with `[2-5]` in the file named `snom_3xx_dialplan_usa3.xml` (assuming you are using a snom phone).

```
<?xml version="1.0" encoding="utf-8" ?>
- <dialplan>
    <template match="1.........." timeout="0" user="phone" />
    <template match="[2-7].." timeout="0" user="phone" />
    <template match="8[2-7].." timeout="0" user="phone" />
    <template match="[2-9]11" timeout="0" user="phone" />
  </dialplan>
```

- **Authentication User/Password:** This setting makes it easier to carry out domain level settings of phones. Using this setting, the administrator can create identical user names and passwords for all devices in a domain. This password will bypass users' passwords. However, an extension@domain is still required. The default user name is `admin`, and the default password is `password`.
- **Authentication PIN:** This setting allows you to override the user's PIN, which is used on the phone itself. Administrative access to the phone allows you to reset the phone.

Domain Address Book

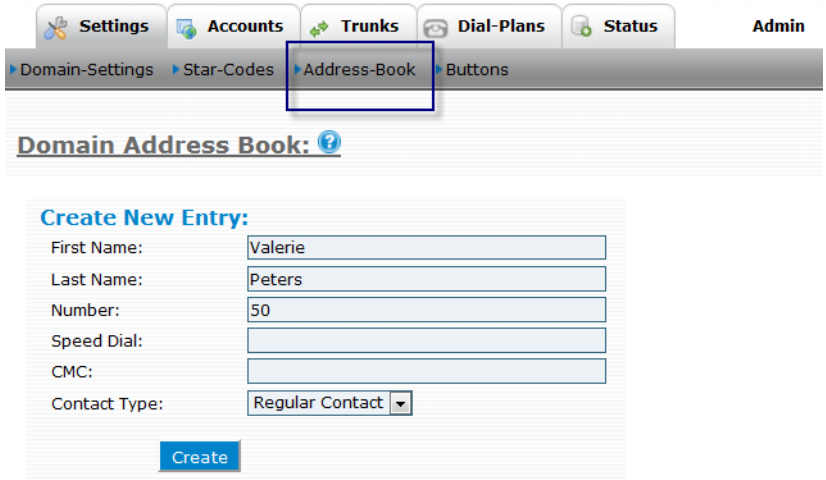
The domain address book allows users on the same domain to easily call each other and to see who's calling. Users can search for contacts from either the web interface or from

their IP phones. From the address book, contacts can be whitelisted or blacklisted and CMC codes can be added to a contact's information.

Creating a Domain Address Book

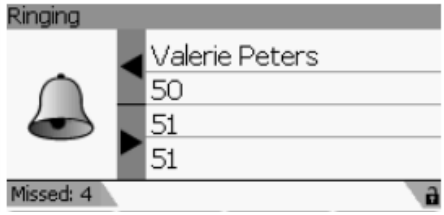
Adding Contacts Manually

Enter the contact's information into the **Create New Entry** form shown below:



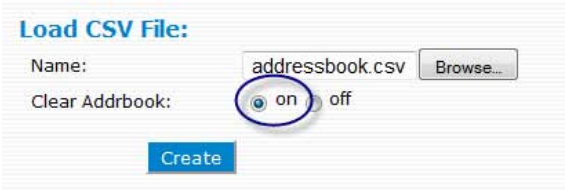
- **Number**: The telephone number of the contact. This is not a SIP URI.
- **Speed Dial**: You may use a two-digit star code to speed-dial this contact. Note that these star codes cannot overlap with any of the standard **star codes**.
- **CMC**: The CMC identifies the customer in the CDR report and is used to expedite billing in offices that bill their clients for phone calls, such as law offices and other businesses that track time spent with clients. As long as the CMC has been added to the address book and the caller is calling from the phone number that is associated with that CMC, the CMC will automatically appear in the CDR report. The CMC can also be entered directly into the display of the phone (by pressing the CMC soft key) if the person is calling from a number other than the number that is in the address book.
- **Contact Type**: The **Contact Type** dropdown allows you to blacklist or whitelist a contact.

Once contacts have been added to the domain address book, their information will be displayed to the person they are trying to reach.



Adding Contacts Using CSV Files

Domain address books can also be compiled through CSV files (see Appendix A). When importing a CSV file, you have to option of clearing existing contacts out of the system before importing new ones.



Adding Contacts Automatically

Contacts who call into an agent group can automatically be added to the address book (see **Add to the address book** on page 232).

Adding Contacts by Modifying DID Information

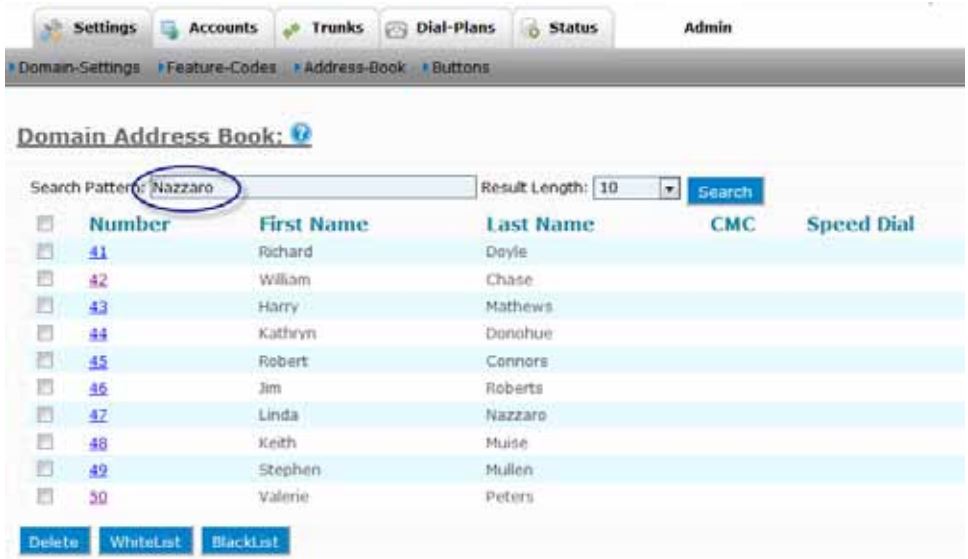
When the system has been configured to automatically add agent group callers to the address book, the caller's DID will be added to the list of address book entries. Using this information, the system can route repeat callers to the same agent. However, agents will be unable to identify the caller unless the contact's information is added to the address book.

1. Click the contact's DID.
2. Enter the contact's information in the **Edit Address Book Entry** form.

Searching for Contacts

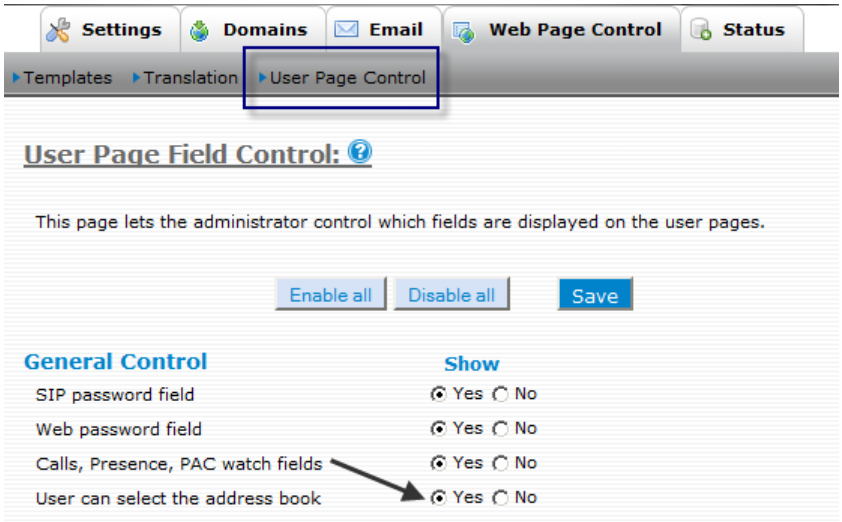
Web Interface

Users can search for contacts by entering the contact's first or last name into the search box:



Phone Display

If the administrator has enabled the **User can select the address book setting** (**Admin > Web Page Control > User Page Control),** users can also search through the domain address book from their IP phones:



Chapter 4

TRUNKS

Trunks are used to route calls in and out of the system. When the system receives a call from an extension, it checks to see if another account is being called. It does this by looking at the `To` field of the SIP packet. If it's not another account, then the system consults the dial plan to determine which trunk the call should be routed to (extension-to-extension calls do not require trunks). When the system receives an outside call, it looks at the IP address it came from to see if the IP address is included in the trunks table, and then routes it accordingly.

In the past, trunks were physical lines, and the number of calls that could be placed was limited by the number of lines. Figure 4-1 shows an example of a traditional trunk. In this example, a telephone switch is connected to a corporate private branch exchange (PBX) through one physical T1 line. A separate line (or channel) is needed for each of the 23 calls that are on the PBX.

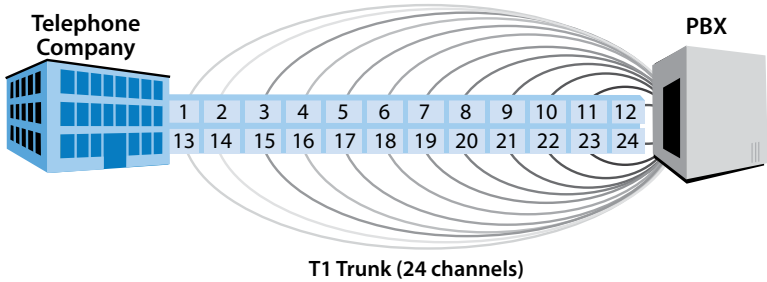


Figure 4-1. Traditional Trunking—Physical Lines (limited by lines)

SIP trunks are virtual lines, so the number of calls that can be made is limited only by bandwidth, rather than actual channels. SIP trunks allow a system to provide access for many individual telephones instead of requiring individual lines for each phone.

Trunks can be dedicated to incoming, outgoing, or two-way traffic. Incoming trunks carry calls into the system from an external network (i.e., PSTN, cellular, ITSP). Outgoing trunks carry calls away from the system to external networks. Two-way trunks can be used for both sending and receiving calls. Figure 4-2 shows a SIP gateway trunk connecting to the PSTN and a SIP registrations trunk connecting to the ITSP.

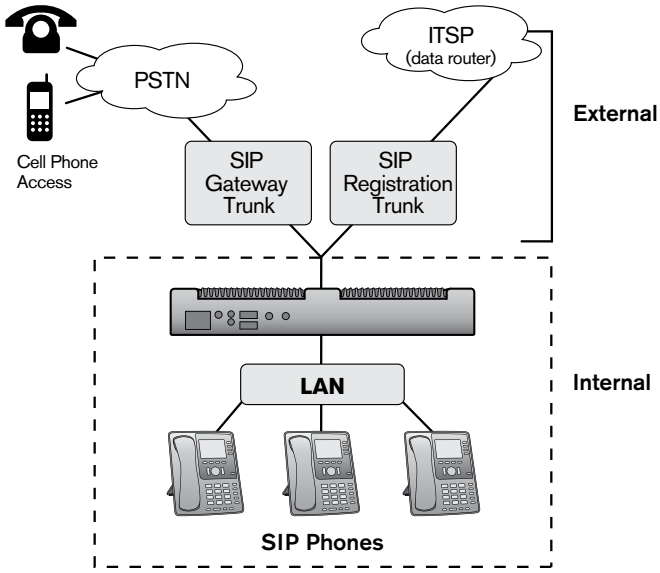


Figure 4-2. Using SIP Trunks for Communicating with External Networks

The snom ONE telephone system has three types of trunks: SIP registrations, SIP gateway, and SIP proxy. All act as an entry and exit point to an external network. The type of network you are connecting to will determine which type of trunk you will need.

Trunk Types

SIP Registrations

When connecting to an ITSP (Internet telephone service provider), you may be required to use a SIP registration trunk due to the fact that the ITSP does not need to

know your public IP address. They will learn it through the registrations process (see Appendix B for information on SIP registration).

The SIP registrations trunk is a popular type of SIP trunk and is easy to set up once the ITSP account has been established. It requires the system to register to the provider, just like an IP phone registers with the system. Like an extension that has been registered with the system, SIP registration trunks require a user name or account (usually the DID), a password, and the IP address or domain name of the SIP or proxy server.

The advantage of the SIP registrations trunk is that the IP address is dynamically bound to the SIP registration, which allows the registration to be used from any IP address. Although service providers often assume that a trunk registration involves an IP phone or an ATA rather than a trunk, many phones can sit behind the snom ONE telephone system and share the resources of the trunk (Figure 4-3). However, most service providers limit the number of calls that can be made over a SIP trunk and use a charging method that simulates the charges accumulated by a physical legacy TDM trunk (i.e., the number of call paths).

Although SIP trunks are virtual trunks and can theoretically have an infinite number of calls, SIP trunks are limited by the amount of bandwidth that is available to handle the calls.

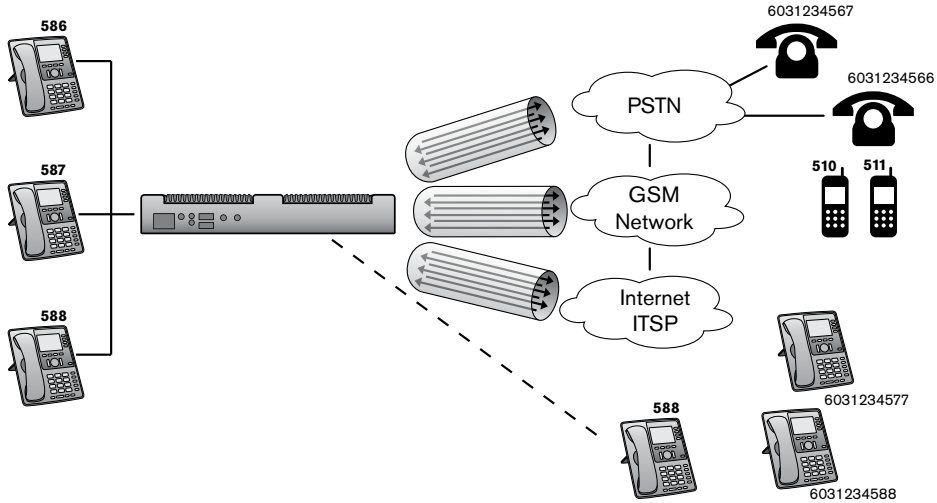


Figure 4-3. SIP Trunks

A SIP registration trunk can also be used to connect two or more snom ONE systems together, as in a branch/head office configuration (see “Connecting Branch Offices Together” on page 142).

SIP Gateway

The gateway trunk is typically used to talk to a PSTN or cellular gateway, which could authenticate the call leg on the IP address in the system. However, some ITSPs that do not have a session boarder controller and require a public IP address use gateway trunks. A gateway is defined as a device that converts media from one network or protocol to another. This type of trunk is used for a media gateway.

SIP gateways are used to transport public switched telephone network (PSTN) terminated signaling across an Internet protocol (IP) network. The gateway sits between the PSTN and the IP network (Figure 4-4). Unlike the SIP registrations trunk, the gateway model does not register—It just sends the traffic to the destination. In this model, the system uses the caller-ID of the system to indicate the extension that initiated the outgoing call (if that extension did not block the caller-ID). This model is typically used with PSTN gateway hardware located on customer premises, but it can also be used to link two snom ONE systems together as long as they are routable to each other, i.e., both are on public IP addresses or on the same private network.

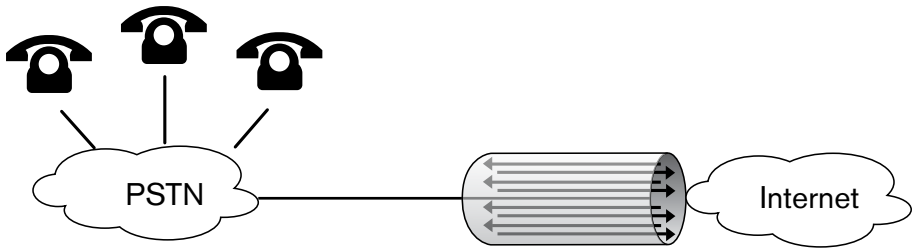


Figure 4-4. Example of SIP Gateway Trunk

Outbound Proxy

The outbound proxy trunk can be used to communicate with any other type of SIP proxy or IP telephone system or to join two IP telephone system deployments together. The outbound proxy trunk is a direct connection to the network and is similar to the gateway model. The difference is in the way anonymous calls are made and in how the

proxy represents its own domain. As the name suggests, the proxy model assumes that you are talking to a SIP proxy or session border controller, while the gateway model assumes you are talking to a SIP user agent. However, the two models are quite similar. As a general rule, use the gateway trunk first, and if you have an issue, try changing the trunk type.

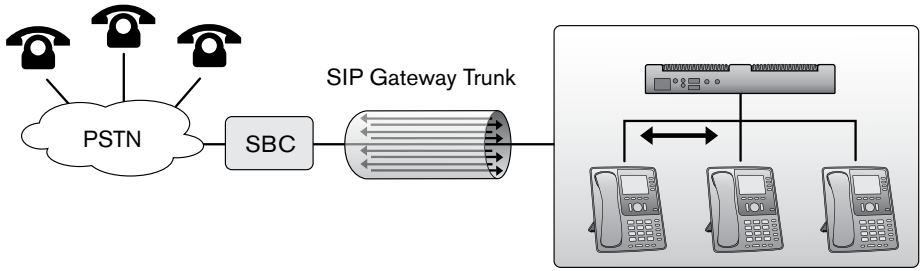


Figure 4-5. Example of Outbound Proxy Trunk

Inbounds Calls

How the System Identifies a Trunk

When a new call comes into the system, the system must determine whether the call is an internal extension or an outside call that is configured to a trunk. To do this, it first looks at the `From` field to see if it matches an extension. If it's not an extension, then from a registration trunk, it looks for a `line` parameter in the SIP INVITE (see Appendix B for information on the SIP INVITE). The `line` parameter is set by the system when the trunk is registered (Figure 4-6). Although it is not a predefined SIP parameter, the `line` parameter is used by many SIP implementations to identify where the call is routed to.

```
REGISTER sip:company.com SIP/2.0
Via: SIP/2.0/UDP 192.168.1.102:1024;branch=z9hG4bK-64g7d07vd6ym;rport
From: "snom ONE" <sip:700@company.com>;tag=5l9bz9udjl
To: "snom ONE" <sip:700@company.com>
Call-ID: 3c26706c531b-5vr6s9jjdbb1
CSeq: 279380 REGISTER
Max-Forwards: 70
Contact: <sip:700@192.168.1.102:1024;line=u4wvf8wz>;reg-id=1;q=1.0;+sip.instance="<urn:uuid:deb7e1bb-c21e-46c2-ab
mobility="fixed";duplex="full";description="snom820";actor="principal";events="dialog";
methods="INVITE,ACK,CANCEL,BYE,REFER,OPTIONS,NOTIFY,SUBSCRIBE,PRACK,MESSAGE,INFO"
User-Agent: snom820/8.1.3
```

Figure 4-6. Line Parameter in REGISTER Request of SIP Trace

```
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.1.102:1024;branch=z9hG4bK-64g7d07vd6ym;rport=1024;received=82.25.93.179
From: "snom ONE" <sip:700@company.com>;tag=5l9bz9udjl
To: "snom ONE" <sip:700@company.com>;tag=5fdc5f3240
Call-ID: 3c26706c531b-5vr6s9jjdbb1
CSeq: 279380 REGISTER
Contact: <sip:700@192.168.1.102:1024;line=u4wvf8wz>;expires=32
Content-Length: 0
```

Figure 4-7. Line Parameter in 200 Ok of SIP Trace

```
INVITE sip:01234567890@company.com;user=phone SIP/2.0
v: SIP/2.0/UDP 192.168.1.11:1024;branch=z9hG4bK-tdrdjojanlk4;rport
f: "snom UK" <sip:700@company.com>;tag=k80fnq9cao
t: <sip:01234567890@company.com;user=phone>
i: 3c2ce782bbbd-d2lwcqymny6i
CSeq: 1 INVITE
Max-Forwards: 70
m: <sip:700@192.168.1.11:1024;line=eeb7fe02>;reg-id=1
X-Serialnumber: 000413400E7C
P-Key-Flags: resolution="31x13", keys="4"
User-Agent: snom820/8.2.35
```

Figure 4-8. Line Parameter in INVITE of SIP Trace

For gateways and proxies, this method is not possible, so if the `line` parameter isn't there to give clues on how to route the call, the system must continue searching the trunk. This is done by a recursive DNS-resolution of the outbound proxy of the trunk. As the system searches, it uses the priority shown in Figure 4-9.

Note: The domain name `localhost` matches any domain name presented in the Request-URI. (The Request-URI is a Uniform Resource Identifier that lists the user or service to which the request is being addressed.) Also, if the `From` header identifies an extension on the system, the trunk identification will be cancelled and the system will assume that the call is from that extension, regardless of whether the extension is registered on the perceived IP address or not. The system will then try to authenticate the extension and determine which IP addresses and ports a trunk may send requests to.

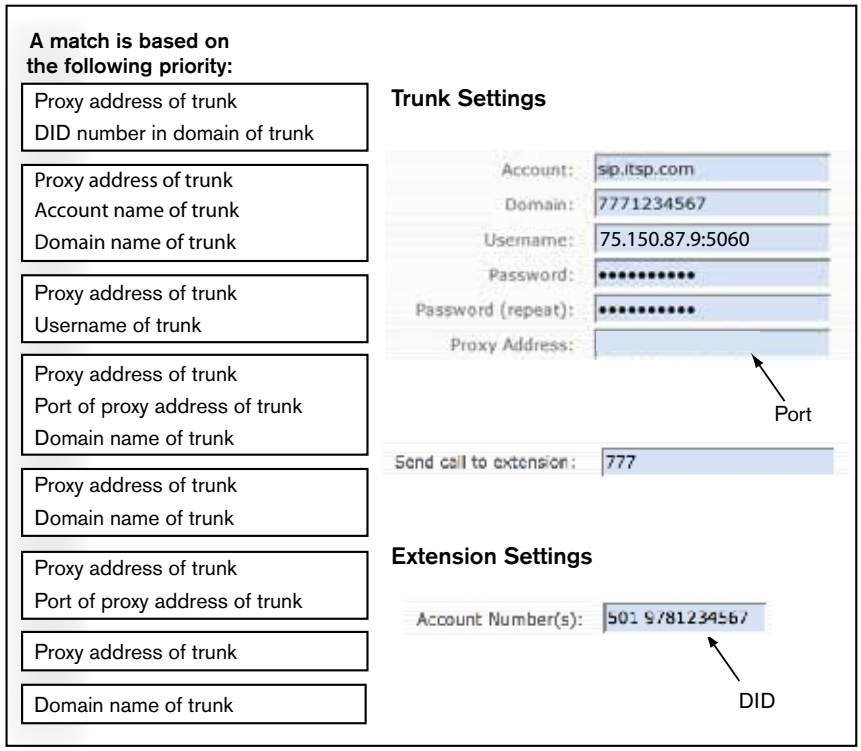


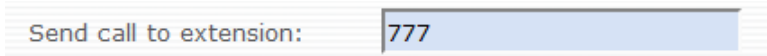
Figure 4-9. Identifying Gateway and Proxy Trunks

How the System Routes a Call to the Proper Extension

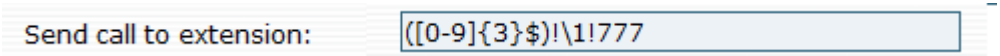
Basic Routing

Once the trunk has been identified and the inbound call is trusted, the system must determine where in the system to send the call. Two possibilities are available for this:

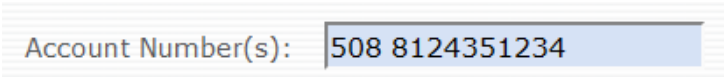
1. The system first looks at the trunk's **Send call to extension** setting. If the setting includes an extension, the call will be sent to that account. If the extension does not exist, the call will fail.



If the setting includes regular expressions, the system will route the call accordingly (see "When Regular Expressions are Involved" on page 121). When using regular expressions in the **Send call to extension** field, it is important to provide a default extension in the event the replacement pattern does not produce an existing extension (in the example shown below, 777 is the fallback extension).



2. If nothing was set in the trunk's **Send call to extension** setting, the system must go to the individual extensions to determine whether the called number is associated with any account. Using the example shown below, if the number dialed was `8124351234`, the system will see that extension 508 is associated with the incoming number and will route the call accordingly. If no extension is associated with the incoming number, the call will fail.



The number shown to the right of the extension is known as a DID. This method of attaching a DID to an extension is a viable routing method only when the number of DIDs is small (e.g., four to ten DIDs). When a large number of DIDs are involved, using regular expressions in the trunk's **Send call to extension** field is a better approach (page 121).

Corresponding Log File and SIP Trace

This section provides a few SIP traces that correspond to the settings shown in the previous section ("Basic Routing"). When a call has been routed to an extension through the **Send call to extension** setting, the system writes a log (Figure 4-10) with the message `Trunk <name> sends call to ...` into the log file (log level 5).

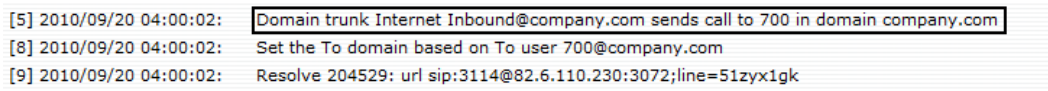

[5] 2010/09/20 04:00:02: Domain trunk Internet Inbound@company.com sends call to 700 in domain company.com
[8] 2010/09/20 04:00:02: Set the To domain based on To user 700@company.com
[9] 2010/09/20 04:00:02: Resolve 204529: url sip:3114@82.6.110.230:3072;line=51zyx1gk

Figure 4-10. Log File Reflecting "Call to extension" Setting

If the trunk's **Send call to extension** field is empty and the system finds an extension that is associated with the number that was called, the called number will be reflected in the user portion of the Request-URI is `8124351234` (Figure 4-11):

```
INVITE sip:01133503115@company.com SIP/2.0
Record-Route: <sip:255.255.255.255;lr=on;ftag=47367AFC-2197>
Via: SIP/2.0/UDP 255.255.255.255;branch=z9hG4bK62c.4abb5c4.0
Via: SIP/2.0/UDP 255.255.255.255:5060;branch=z9hG4bK1EF8C71F8C
Remote-Party-ID: <01223456789@255.255.255.255>;party=calling;screen=yes;privacy=off
From: "01223456789" <sip:01223456789@255.255.255.255>;tag=47367AFC-2197
To: <sip:441133503115@n.e164.org.uk>
Date: Mon, 20 Sep 2010 08:02:11 gmt
Call-ID: 34F55FE2-C3C411DF-B554F206-159454F0@255.255.255.255
Supported: timer,resource-priority,replaces
Min-SE: 1800
User-Agent: ITSP
Allow: INVITE, BYE, CANCEL, ACK
CSeq: 101 INVITE
Max-Forwards: 14
Timestamp: 1284969731
Contact: <sip:01223456789@255.255.255.255:5060>
```

Figure 4-11. SIP INVITE Reflecting DID Routing

When Regular Expressions are Involved

Regular expressions can be used for numerous call routing purposes, but they are especially helpful when you have a large number of DIDs. When you have a few DIDs, you can simply enter the DID number into the **Account Number(s)** setting in the extension that the DID is assigned to. Assigning a large number of DIDs to individual extension accounts, however, is cumbersome and can be expedited through the use of regular expressions (direction inward dialing is discussed on page 124).

A regular expression is a special character string that describes a search pattern that the trunk will use when looking for a match for an incoming number. The expression consists of the following key elements:

- **Pattern**: The pattern portion of the string defines the numbers that the system will use when searching for a match and *how many*. In the example shown in Figure 4-12 (expression 1), the system will consider all numbers (0 through 9) when identifying a match and will include only the first seven digits. In expression 2, the system will still consider all numbers but will include only the last three digits.

- **Replacement**: The replacement field tells the system which expression to use when dialing. In our example, expression 2 has been defined (as is indicated by `\2`), so if `9781234567` had been the incoming number, `567` would be dialed.
- The Request-URI (`To` header flag): This flag tells the system where to look. By default, the system will look at the Request-URI ("u"). However, if you want the system to look at the `To` header, use a `t` as shown in Figure 4-14 (some Internet service providers provide the destination information in the `To` header). SIP recommends the Request-URI.
- Delimiters (field separators): Each part must be separated by a delimiter (a unique character which is not used elsewhere in the setting string). In the example shown in Figure 4-12, an exclamation mark has been used.

Note: Expressions are written without any spaces: `![0-9]{7}([0-9]{3}$)!\1!`

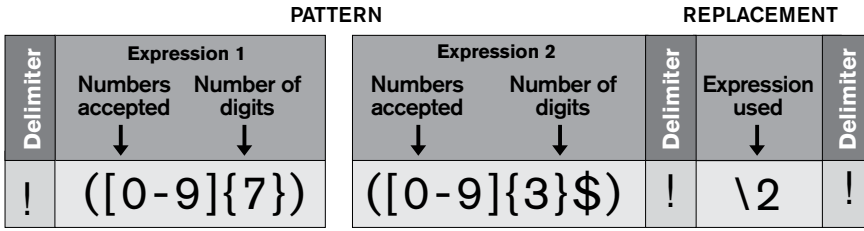


Figure 4-12. Regular Expressions String—Multiple Expressions

Important: The example shown in Figure 4-12 simply shows that numerous expressions can be used in one string; however, a single expression in many cases would be sufficient. For example, to specify that only the last three digits of a number should be used for dialing, you could use `!([0-9]{3}$)!\1` as shown in Figure 4-13:

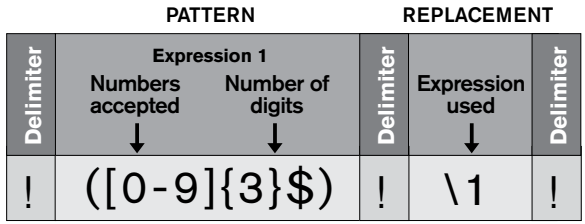


Figure 4-13. Regular Expressions String—a Single Expression

This expression allows the trunk to find the correct extension when lots of DIDs are used on the system. As a safety net, you can also direct the trunk to send the call to a default extension in the event the replacement pattern does not produce an existing extension. The string shown in Figure 4-14 includes a default extension number (777), so if the trunk is unable to find an extension using the replacement field, extension 777 will be called.

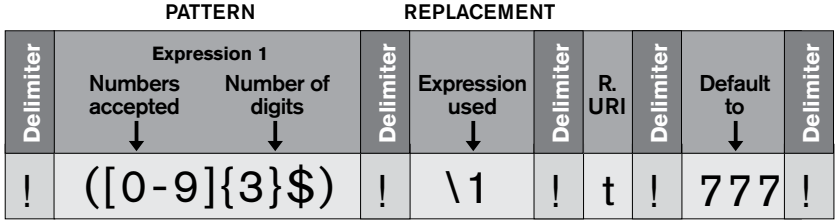


Figure 4-14. Regular Expressions String—Default Extension

Regular Expression Syntax

The syntax used in expressions is explained in Table 4-1:

Table 4-1. Syntax Used in Expressions

Syntax	Function
!	Delimiter (separates each part)
[ ]	Lists the digits that are accepted
{ }	Defines the number of digits
( )	Stores the numbers that match
\2	Indicates which expression to call
*	Wild card (any length and character)
$	Tells the system to read from end of string

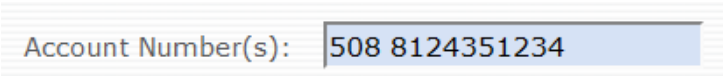
Samples of regular expressions are shown in Table 4-2.

Table 4-2. Examples of Regular Expressions

Example 1	`![0-9]{7}([0-9]*)!\1!t!100` This example is common in Europe. It is used to strip the main number of the system so that the remaining numbers can be used to identify the extension. If the extension is not found, the call will be sent to the auto attendant. This example assumes that the number starts with 7 digits (e.g., 0228123) and that the auto attendant is located on extension 100.
Example 2	`!([0-9]{4}$)!\1!t!100` This example always uses the last 4 digits of the number, regardless of how long the number is. This example assumes that the number of digits is always the same.
Example 3	`100` This example is common in U.S. offices, where it is typical to send all calls to an auto attendant. This example assumes that the auto attendant is located on account 100.
Example 4	`!1([0-9]*)!\1!u!100` This example can be used to strip the first digit from a DID number (default destination would be 100).

Regular Expressions and Direct Inward Dialing (DID)

Direct Inward Dialing (DID) allows users on your system to have their own (or even multiple) local numbers assigned to them. With DIDs, anyone outside the company can call the user's unique phone number and reach the user on the same phone as those who dial the user's extension number internally. Before you can use DID numbers, you will need to purchase them from a DID service provider, then link the DID numbers to the extension accounts. The easiest way of doing this is by entering the DID number into the **Account Number(s)** setting of the extension that will be using the DID.



Though easy to use, this method is cumbersome to employ for a large number of DIDs, so you will need to use an alternate method. The method chosen will depend on the numbering scheme of the DID numbers themselves. When the ending digits of the DIDs form a definite pattern that can lend itself to correlate with extension numbers, you simply need to enter a single string into the trunk's **Send call to extension** field. The only requirement here is that the ending digits must begin with a 4 or higher (extension numbers should stay within the range from 4xx through 7xx to keep from overlapping with **Direct Destinations** numbers).

If the last 3 or 4 digits of a block of DIDs begin with a 1, 2, or 3 (e.g., 100, 101, etc.), the ending digits cannot be used as the extension numbers. You will need to use the workaround shown in Option 2.

Option 1: Clear pattern with a start number of 4 or higher

If you have a batch of DID numbers with a usable pattern on the ending digits, you can easily use regular expressions in the **Send call to extension** setting. The system will replace the 10-digit DID with the extension number. Table 4-3 displays a list of DIDs that can be easily converted to 3- and 4-digit extensions using regular expressions.

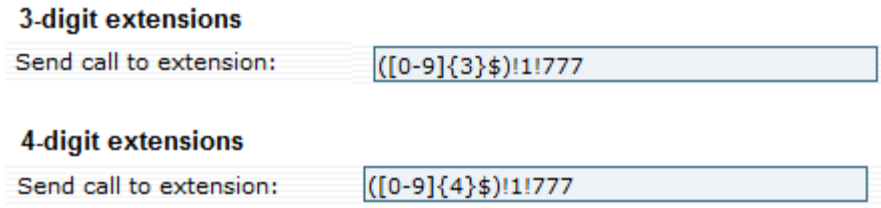
Table 4-3. Direct Inward Dialing Numbers with Usable Patterns

DIDs and 3-Digit Extensions	DIDs and 4-Digit Extensions
978 521-1**400**	978 521-**4100**
978 521-1**401**	978 521-**4101**
978 521-1**402**	978 521-**4102**
978 521-1**403**	978 521-**4103**
978 521-1**404**	978 521-**4104**
978 521-1**405**	978 521-**4105**

Follow the steps below:

1. Create the regular expression.
2. Place the string into the trunk's **Send call to extension** setting.

Using the example shown below, the system will use either the last 3 or 4 digits of the 10-digit number, depending upon which string is used. (If the system cannot find a matching DID, the call will be sent to extension 777.)



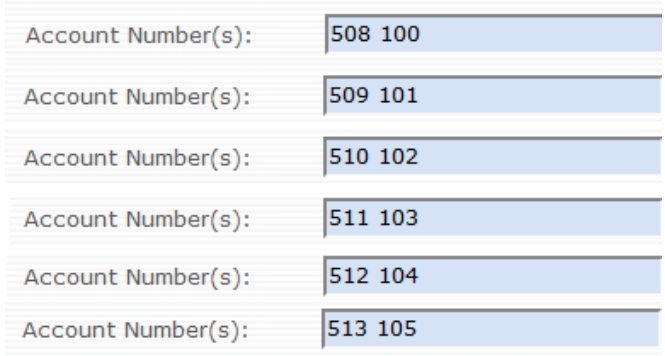
Option 2: Defined pattern with a start number lower than 4

When DID ending patterns are in the 100, 200, or 300 range, you should not create extensions based on these numbers (extensions should begin with 4 or higher). As a workaround, you will need to create aliases for the extensions, and to save time, this should be done when you create the extensions. Once this is complete, a regular expression must be entered into the **Send call to extension** field so that the system will replace the 10-digit DID with the alias number:

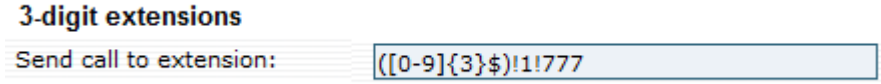
1. Decide which alias numbers to use.

DID	Alias
978 521-1100	100
978 521-1101	101
978 521-1102	102
978 521-1103	103
978 521-1104	104
978 521-1105	105

2. Enter the aliases into the corresponding extension accounts:


Account Number(s): 508 100
Account Number(s): 509 101
Account Number(s): 510 102
Account Number(s): 511 103
Account Number(s): 512 104
Account Number(s): 513 105

3. Enter a regular expression into the **Send call to extension** setting, telling the system to replace the 10-digit DID with the alias number that is associated with the extension account.



Outbound Calls

Caller-ID

The caller-ID is shown in the called party's telephone display and is also used by the carrier for billing purposes. This is typically the `From` field of the SIP packet. When the system sends a call to a trunk, it presents the source of the call, usually the caller-ID of the calling extension. However, in cases of redirected calls, it can get more complicated. Here, the original caller-ID should be in the display of the called party, while for billing purposes, a local identity on the system must be used.

Also, in many cases, it is necessary to translate a local number (e.g., `sip:123@localhost`) into a global telephone number (e.g., `sip:9781234567@itsp.com;user=phone`). The `user=phone` parameter indicates that the domain name should be ignored when presenting this number. This number is also known as the ANI (automatic number identification).

Generating the ANI

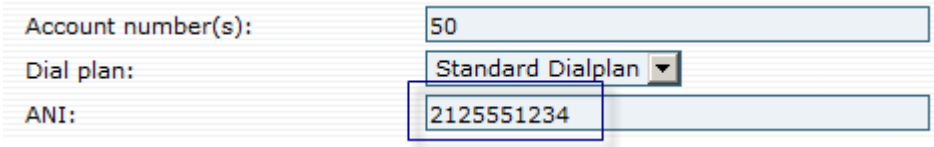
An ANI is an administrative number provided by the system to identify the caller to the receiver and is not necessarily the originating number. Before the system can generate an outbound call on a trunk, it must have an ANI. To get the ANI, the system first checks the SIP URI in the `To/From` header and the identity headers (`P-Preferred-Identity`, `P-Asserted-Identity` or `Remote-Party-ID`) for the `user=phone` flag. When this flag is set, those numbers will be used as the ANI.

```
INVITE sip:01234567890@company.com;user=phone SIP/2.0
v: SIP/2.0/UDP 192.168.1.11:1024;branch=z9hG4bK-tdrdjojanlk4;rport
f: "snom UK" <sip:700@company.com>;tag=k80fnq9cao
t: <sip:01234567890@company.com;user=phone>
i: 3c2ce782bbbd-d2lwcqymny6i
CSeq: 1 INVITE
Max-Forwards: 70
m: <sip:700@192.168.1.11:1024;line=eeb7fe02>;reg-id=1
X-Serialnumber: 000413400E7C
P-Key-Flags: resolution="31x13", keys="4"
User-Agent: snom820/8.2.35
Accept: application/sdp
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUBSCRIBE, PRACK, MESSAGE, INFO, UPDATE
Allow-Events: talk, hold, refer, call-info
```

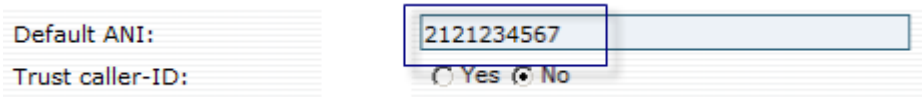
Figure 4-15. ANI and `user=phone` Flag

However, if the SIP URI does not contain the `user=phone` flag, the system looks for the ANI from the following places (in the order listed here):

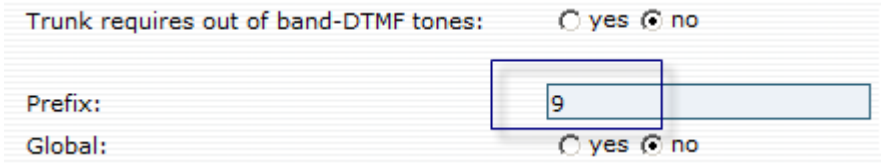
1. Extension account (**ANI** setting): If the local account has an ANI number, the system uses this number. Every extension, or any other account that has a dial plan, also has an ANI number field. By entering this information, it is clear how this account will be presented to the outside world.



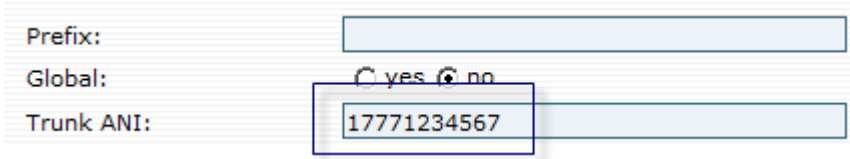
2. Domain (**Default ANI** setting):



3. Trunk (**Prefix** setting): If the trunk's ANI has not been set, the system will check to see whether a prefix has been set in the trunk. When this is the case, the system will add the fixed number to the front of all calls leaving the trunk. In many cases when you have an ITSP, you may want a prefix number to be appended to the front of all calls. The prefix could be an account number, a least-cost routing number, or a number to indicate an outside line on another system (e.g., 9 as shown below).



4. Trunk (**Trunk ANI** setting).



As a last resort, the system uses the DID number of the trunk, if there is one. This is a typical scenario in the NANPA area, where a trunk has a primary number associated with it. When someone calls the number, the caller will typically reach an auto attendant that processes the DID number.

Representing the Source

The system differentiates between the following two numbers when presenting a number on the trunk.

- Display number: This number is the number that the user should see on the display of the phone. In the case of a redirected call, this number would be the original caller-ID that the system sees on the incoming call.
- Network number: This number is the number that the provider wants to see for billing purpose.

Over the last few years, providers have developed different methods of representing these two numbers:

- RFC 3325 describes a way to represent these two numbers. In most cases, it makes sense to use the `P-Asserted-Identity` header. In this case, the `From` header in the INVITE represents the display number, while the `P-Asserted-Identity` header has the network number. A similar representation can be done with the `P-Preferred-Identity` header. The system changes only the name of the header from `P-Asserted-Identity` to `P-Preferred-Identity`. The rest remains the same, as in the first method.
- No Indication: This method simply discards the display number and uses only the network number in the `From` header. This method is a fallback when the provider cannot handle any other method. The disadvantage here is clearly that any redirection information gets lost.
- Remote-Party-ID: This method is described in a draft that expired years ago; however, there is still a lot of equipment outside that is supporting this method. In this case, the `From` header in the INVITE represents the network number, while the `P-Asserted-Identity` header is the display number.
- RFC 3325, but don't hide: This method should not be used. It has been used in environments where the fields have gotten mixed up, and it is creating even more confusion.
- To strip the first digit from a DID number, you can use the pattern `!1([0-9]*)!\1!u!100` (default destination would be 100).

Creating Trunks

This procedure shows you how to create trunks.

1. From the domain where the trunk will be used, click the **Trunks** tab.
2. Enter a name for the trunk. You can name the trunk anything you prefer (e.g., company name, department, etc.). The name must consist of alphanumeric characters and may contain spaces.

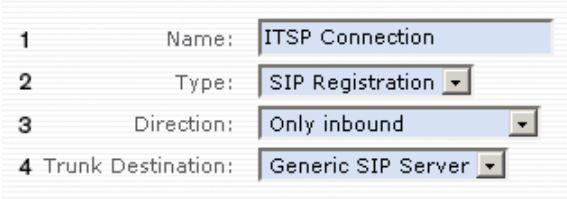
3. From the dropdown list, choose a trunk type. (For a description on each trunk type, see "Trunk Types" on page 114.)
4. Click **Create**.

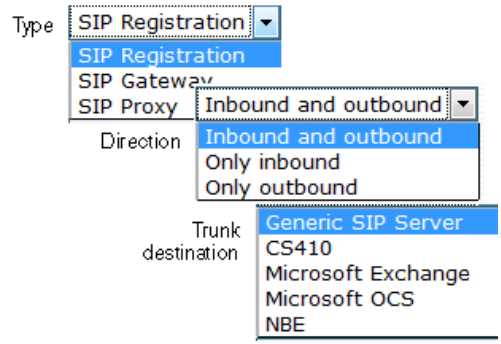
The following section shows you how to configure the trunk settings.

Configuring Trunks

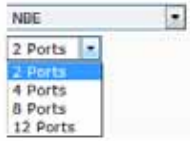
General Settings

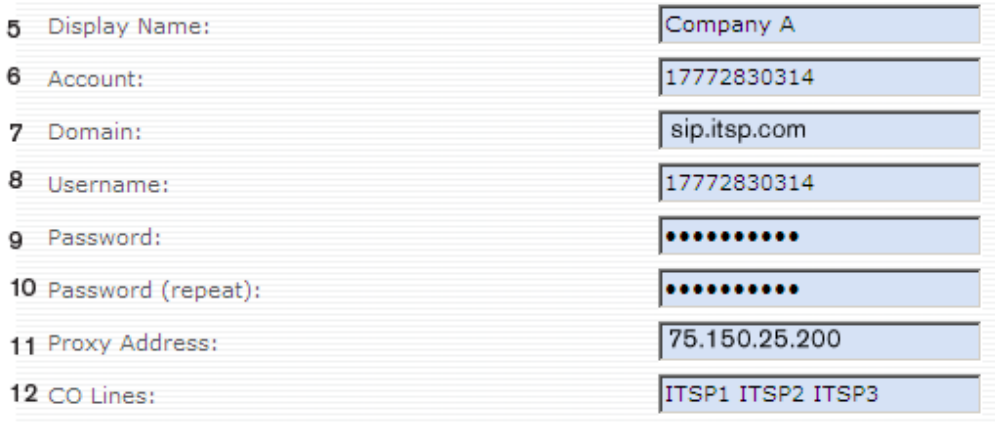
Trunks have a large number of settings. For an explanation of each setting, match the numbers in the image with the numbers below the image.





1. **Name:** This setting allows you to name the trunk (the name and type of trunk can be changed at any time).
2. **Type:** See "Trunk Types" on page 114.
3. **Direction:** Traffic can be limited to either inbound traffic or outbound traffic.
   - Inbound and outbound: Typical setting.
   - Inbound only: Limiting traffic to inbound traffic prevents users from using the trunk for unauthorized calls.
   - Outbound only: Enable this setting if you are using a trunk for outbound traffic only. It makes it easier for the system, as the trunk will not try to match inbound traffic to this trunk.
4. **Trunk Destination:** This setting is useful when connecting to an Exchange server. Depending upon the setting, the SIP headers will be altered. If NBE is selected, additional options are made available (2, 4, 8, or 12 ports).





5. **Display Name:** The display name is used for display purposes in the trunk listings page. This setting is the friendly name of the SIP `From` field and can be changed at any time.

6. **Account:** The account is typically the main DID on the trunk.
7. **Domain:** The domain is typically the upstream registration server or SIP server. It can be an IP address or a domain name.

   Example: `sip.itsp.com`

   If the service provider is using DNS SRV records, it could be itsp.com.
8. **Username:** The user name and password are used for authentication purposes (not all registrars require a different username for authentication).
9. **Password:** The password needs to match the password from the trunk provider.
10. **Password (repeat):** Confirmation of the password.
11. **Proxy Address:** This setting defines where requests that are made of this trunk will be sent. When this field is set, requests will be sent to the specified address. Otherwise, the dial plan replacement field will be used to route the request.

    Example: `sip.messagenet.it:5061`

    The outbound proxy field follows the definitions of RFC 3263 ("Locating SIP Servers"). You may use the fully qualified domain name (FQDN) for a SIP server. If you add a colon with the port number after the FQDN DNS, a resolution will be used; otherwise, the system will try DNS NAPTR and DNS SRV first. You can force the SIP connection to use TCP by supplying an outbound proxy.

    Example: `sip:hostname:5060;transport=tcp`

    Important: The outbound proxy is an important setting. If an outbound proxy is not used, then the system will assume that SIP requests on this trunk can come from any location. This will make it difficult for the system to match incoming SIP requests. Unless you want to receive requests from any location on the Internet, you should specify an outbound proxy.
12. **CO (central office) Lines:** CO-lines can serve multiple purposes on the system. They allow you to channelize a trunk and can be used in a way similar to the CO-lines of traditional TDM-based PBX systems. Although snom ONE runs calls through SIP trunks over computer networks instead of connecting to

public telephone lines (at least directly), CO-lines are still useful for determining which calls are active between the system and the outside world.

To begin with, each trunk may have several CO-lines, and because users can subscribe to the state of CO-lines, each CO-line name must be unique within a domain. For example, four CO-lines might be set up on trunk 1 with the names `co1 co2 co3 co4`, while trunk 2 might contain `co5 co6 co7 co8` (the list must be delimited by spaces). The system will reject names for CO-lines that are already in use by accounts or other CO-lines in the same domain. With regard to monitoring, the CO-lines that you establish can be monitored from the domain's Account list. If a CO-line is in use, it will display the extension and the outside phone number to which it is connected.

CO-Line Use

Limiting inbound and outbound traffic: CO-lines can be used to limit the number of calls that can be assigned to a trunk. When the CO-line setting is used, the system will reserve one line for each call. When all lines are in use, the system will reject further calls that attempt to use the CO-line. For example, if you have a SIP trunk that can handle only three simultaneous calls, you should assign three CO-lines (e.g., `co1 co2 co3`). If a fourth simultaneous call attempt is made, the system will play a fast busy signal. If you have more than one trunk, you can set up a failover behavior so that the system will try to use a different trunk for the call once the first trunk has all CO-lines in use.

Reserving lines: If you want to reserve lines exclusively for inbound traffic, put a `:i` after the line name. The system will use that line only for inbound traffic (e.g., `line1:i`). If you put a `:o` after the line name, the system will use that line only for outbound traffic. If there is no attribute set after the colon, the line will be available for both inbound and outbound traffic.

Monitoring CO-lines: CO-lines are required for many basic functions. In most small offices, transfers are done by pressing the **Hold** key and lighting the lamps on the other phones. In order to do this, the phone must be able to display which call is on which CO-line.

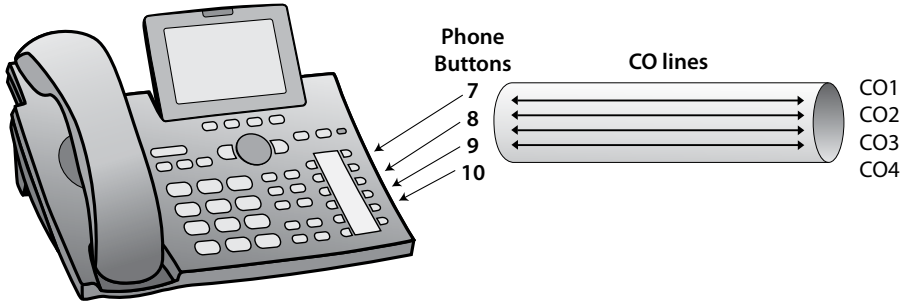


Figure 4-16. CO-Lines Linked to Phone Buttons

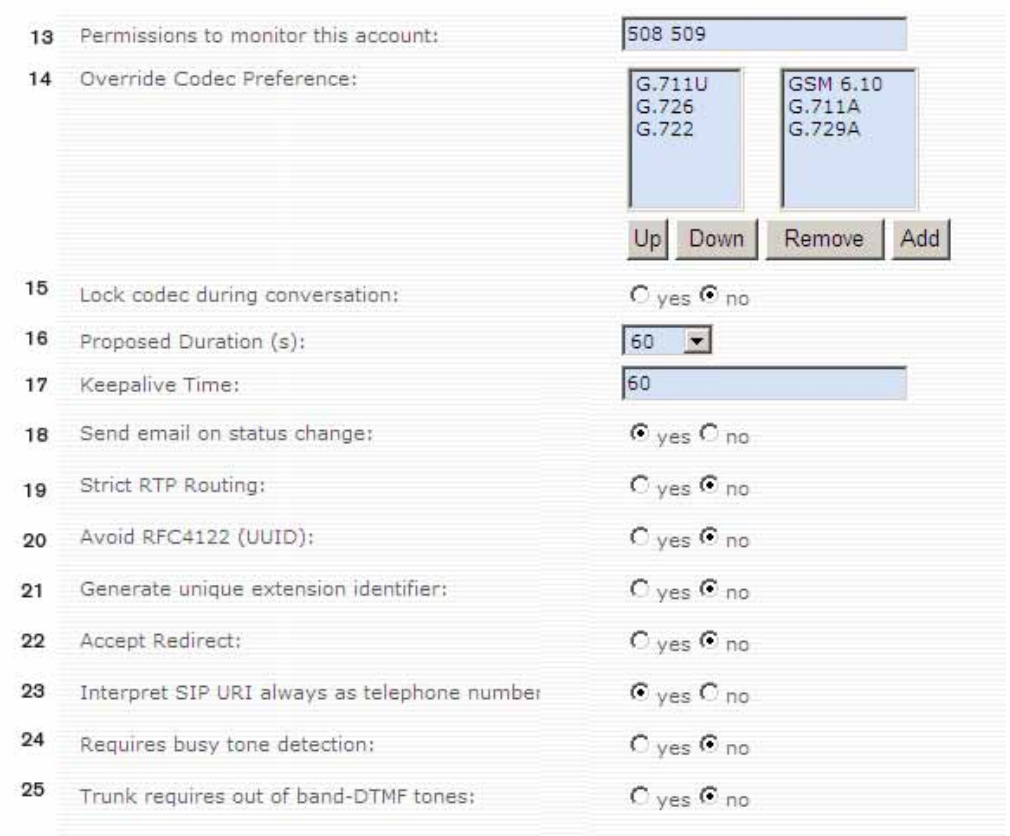
From a system point of view, the status of a CO-line is similar to the status of an extension: It may be idle, connected, ringing, or on hold. It also might be holding a parked call. Therefore, the mechanism that shows the status of a CO-line is similar to the mechanism that shows the status of an extension. This implies that the name of the CO-line must not clash with the name of an extension or any other account on the system. (To be able to see the CO-line status, the user agent needs to subscribe to the status of the CO-line. See the description of the phones on how to do this.)

13. **Permissions to monitor this account:** Enter the extensions that are permitted to monitor this account.

14. **Override codec preference:** Use this setting to specify particular codec preferences for the trunk. By default, the system uses the codec preference of the system, which has the advantage of allowing the system to negotiate codecs in such a way that transcoding can be avoided. (When default mode is used, no codecs will be displayed on the left side of the codec selection box.)

    If it is necessary to enforce specific codecs on a trunk, choose a codec from the list of available codecs and click the **Add** button. Repeat as needed. Be sure to position the codec with the highest preference first. To delete a codec, click the **Remove** button. To move a codec up or down in the preference list, use the **Up** and **Down** buttons.

15. **Lock codec during conversation:** Locking the codec prevents someone from switching codecs in mid-conversation and ensures that the user agent continues to send and receive media properly. (Some user agents are not capable of changing the media once the conversation begins.) When this setting is used, snom ONE transcodes the stream so that changes made to the codec by the other side go unnoticed by the user agent.



16. **Proposed Duration (s):** Use this setting to specify the registration duration. Although the registrar typically defines the duration of the registration (according to the IETF standards), some providers follow the proposed duration of the trunk. The values range from 20 to 3600 seconds. One hour (3600 seconds) is a reasonable value.

Because some providers will accept the proposed duration without bothering to refresh the NAT binding, you need to force the system to renew the registration in a shorter period of time and ignore the service provider's registration. This is done through the **Keepalive Time** setting below.

17. **Keepalive Time:** Keepalive time is the time required to keep the registration live before it re-registers. This setting helps with trunks that connect to ITSPs that have a good session border controller. This setting may cause a lot of traffic to your service provider, so be sure not to enter an unnecessarily short time. Typically, this setting can be left blank.

18. **Send email on status change:** Once a trunk has been registered, it is critical that status changes are brought to the attention of the appropriate individual. For example, if the service provider goes off line and the trunk looses the registration, the system will send an email notification to the email account that is specified.

19. **Strict RTP Routing:** This setting is needed because the IETF allows "RTP traffic send ports" to be different from "RTP receiving ports," creating an extremely NAT-unfriendly situation. While most implementations today use the same port number for sending and receiving RTP, some gateways still insist on strict IETF compatibility. In such cases, this setting should be enabled. We recommend you keep this flag disabled ("No") unless asymmetrical ports are required.

20. **Avoid RFC 4122 (UUID):** Not all registrars ignore RFC 4122 (UUID) when it does not support it, so it is necessary to explicitly suppress the UUID in register requests. SIP implementations that are not able to deal with UUID report a "Bad Request" to indicate that they were not able to process the request. The UUID is used to indicate that a registration replaces another registration, which is useful for avoiding double registration after a system restart.

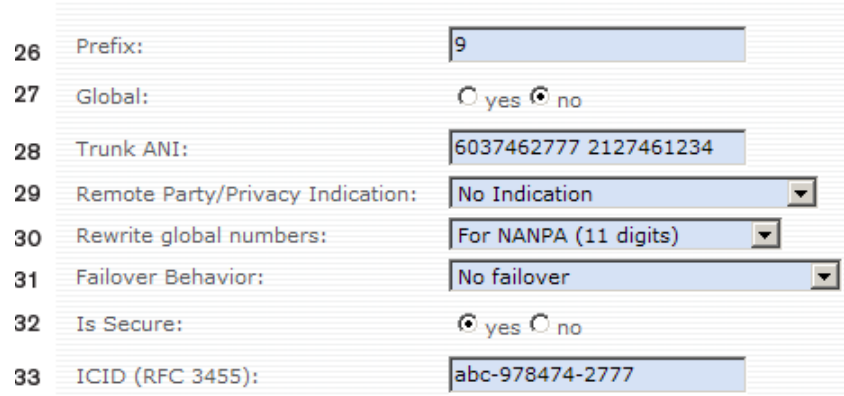
21. **Generate unique extension number:** This setting is used for emergency calls, so that the 911 call center can directly call the extension without having to go through the auto attendant. When this setting is set on the trunk, the system will use the EPID of the extension to represent where the call is coming from. (If it does not exist yet, the system will allocate a new EPID.)

22. **Accept Redirect:** Use this setting if your trunk should respect redirect codes. By default, this introduces significant security risks because the system can-

not determine whether these redirects introduce additional costs (redirection to expensive numbers). Therefore, enable this setting only if you are sure that your service provider or SIP gateway does not abuse this feature. This flag is especially important when you use the system with Microsoft Exchange or other Microsoft products, such as the speech server. Also enable this setting when you have a trunk that comes from another system. This will make it possible to call from one system to another.

23. **Interpret SIP URI always as telephone number:** When a call comes into the system, the system needs to know how to interpret the number. In SIP, the URI contains a domain name; however, in most cases, the domain name should be ignored when interpreting the URI coming from this trunk (because the user portion is just a telephone number). Usually, this is indicated by the parameter "user=phone," but not all service providers set this flag. By turning on the "Interpret SIP URI always as telephone number," you make the system believe that this flag was set on the trunk call.
24. **Requires busy tone detection:** When an analog PSTN gateway (e.g., FXO) is used, hangup detection can be an issue. In FXO, the hangup signal might be just a tone that needs to be detected. Unfortunately, no international standard exists for the disconnect tone. Incoming international calls might give you a disconnect tone that the system has to recognize. Of course, if the PSTN gateway is capable of detecting this, the task should be left to the PSTN gateway. However, as a fallback, you may also configure the system to perform the hangup detection. The disadvantage of doing this is that it costs additional CPU resources, and it might randomly disconnect calls; for example, if the other party plays back a tone that sounds like a busy tone, the call may be disconnected. The best way to avoid these kinds of problems is to use a digital line, e.g., a SIP trunk.
25. **Trunk requires out-of-band DTMF tones:** When this setting is enabled, the trunk will use RFC 2833.

Outbound Settings

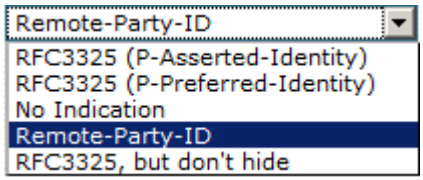

26 Prefix: 9
27 Global: yes no
28 Trunk ANI: 6037462777 2127461234
29 Remote Party/Privacy Indication: No Indication
30 Rewrite global numbers: For NANPA (11 digits)
31 Failover Behavior: No failover
32 Is Secure: yes no
33 ICID (RFC 3455): abc-978474-2777

26. **Prefix:** This setting is used as a representation of the system when making outbound calls. The system will add the prefix to the front of all calls leaving the trunk. (See also "Generating the ANI" on page 128.)

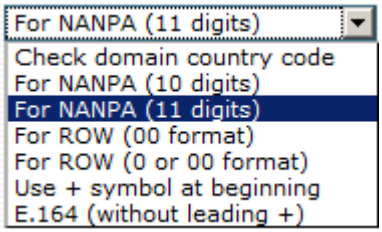
27. **Global:** This setting is used only in multi-domain environments. When it is enabled, calls that come in on this trunk are permitted to jump into other domains if a match is found on a global alias name. (If the direction is not only inbound, then other domains may use this trunk in their dial plans for outbound calls.) When this setting is disabled, the system does not search for tel:-alias names.

28. **Trunk ANI:** You can configure each trunk with an ANI (Automatic Number Identification). ANI is a service that tells the recipient of a telephone call the telephone number of the person making the call. In most cases, the ANI is used in the `From` field in the SIP packets or the caller ID.

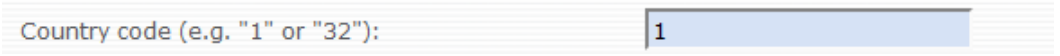
29. **Remote Party/Privacy Indication:** This setting tells the system how to present the caller-ID on the trunk (see "Caller-ID" on page 127).



30. **Rewrite global numbers:** When you are using a trunk, you may have to represent the telephone number in a specific format. For example, in the NANPA area, you might want to use 10 or 11 digits to represent a national number.


For NANPA (11 digits)
Check domain country code
For NANPA (10 digits)
For NANPA (11 digits)
For ROW (00 format)
For ROW (0 or 00 format)
Use + symbol at beginning
E.164 (without leading +)

If you are using several trunks, you can represent the same number in different styles depending on the trunk. The **Rewrite global numbers** setting corresponds to the **Country Code** setting (see page 94):



31. **Failover Behavior:** When the trunk receives an error code, it might send the call back to the dial plan and continue the matching process. The system continues the dial plan with the next highest priority, ignoring entries with lower or same priority. This is useful when the trunk is just a "trial" to place the call. One example is when several PSTN gateways are available for terminating the call and one gateway does not accept any more calls. Another example is when you first try to route the call via a peer-to-peer call using ENUM or other location methods and only if such resolution does not result in a connection fallback to a PSTN call. The setting allows four behaviors:

    - No failover: This is the default behavior. In this case, the caller will receive the error code as a result of the attempted call.
    - On 5xx and 408 error codes: This will trigger failover only when a 5xx or 408 class error code is received. PSTN gateways typically return 5xx class error codes when all channels are in use; however, this mode will allow you to switch to the next PSTN gateway when a line is busy and will not trigger the failover.
    - On all error codes: In this case, all error codes will trigger the failover process. Note that call redirect will also be treated as an error code, as

the redirection destination can easily be abused to route calls through expensive routes.

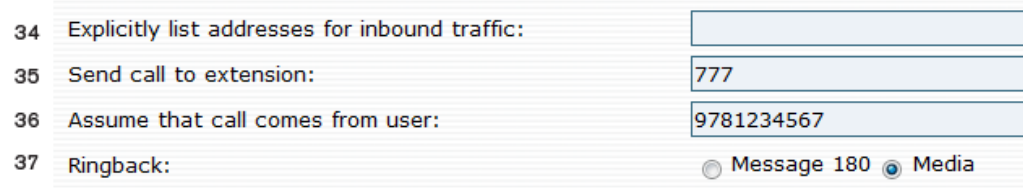
– Always, except for busy response: Even if the remote party is busy, the system will try alternate routes.

If you are using failover, you have the option to specify a request timeout value for the trunk. By default, this is 32 seconds (the SIP default request timeout). However, in many cases, it makes sense to specify a shorter value. After the request timeout, the system will internally generate a "408 Request Timeout" response code and process it according to the failover rules.

32. **Is Secure:** This setting is used to indicate that outbound calls on the trunk can be treated as secure calls. For example, when the trunk goes to a local PSTN gateway, you might decide to treat this call as a secure call. Incoming calls with the SIPS scheme will ask the snom ONE system to ensure that the call be kept secure end-to-end.

33. **ICID (RFC 3455):** This setting is used in the IMS environment and is sent in the `P-Charging-Vector` header of the SIP packets on the trunk. It is essentially a token that identifies the trunk. If your provider uses this header, it should be placed into this field.

Inbound Settings



34. **Explicitly list addresses for inbound traffic:** This setting allows you to explicitly state trusted inbound proxy addresses and enables you to identify the origin of the request. It is ideal for VPN environments or when routing calls between offices, as it allows you to create a single trunk and specify the IP addresses of the other locations. The addresses can be either IP addresses (with an optional port number behind) or a DNS A or AAAA address.

35. **Send call to extension:** This setting is discussed in "Inbound Calls" on page 117.
36. **Assume that call comes from user:** This setting is used for trunks that accept redirects. The settings must be an extension in the domain of the trunk. This setting is necessary in order to determine what dial plan to use, and it is also necessary to charge a user on the system for the call. For regular trunks, you should leave this field empty.
37. **Ringback:** This feature was introduced to deal with network operators who were unable to deal with early media. Although using the 180 Message simplifies the signaling in forking calls scenarios, it creates additional delay when the called party picks the handset up and the first samples on the conversion may not be transported. We strongly recommend leaving the flag set to **Media** (which is default) and asking the operator to fix the problems with early media.

Connecting Branch Offices Together

This section describes how to connect two snom ONE systems together so that calls between the two locations will be routed through VoIP rather than through the local PSTN. Two different scenarios are presented:

- Two snom ONE telephone systems with public routable IP addresses (this model is also suitable for two systems on a private network with no NAT issues)
- Two snom ONE telephone systems: A head office site and a remote site

Using a Gateway Trunk

SIP gateway trunks are the best method for connecting two snom ONE telephone systems, as long as both systems either have public routable IP addresses or are on a private network with no issues with NAT. Likely candidates for this configuration are the classroom environment and organizations with a large private network (as long as the system has an interface directly on a public IP address). Figure 4-17 shows two remote sites connected by two gateways. Callers from either system can dial the other system using four-digit dialing.

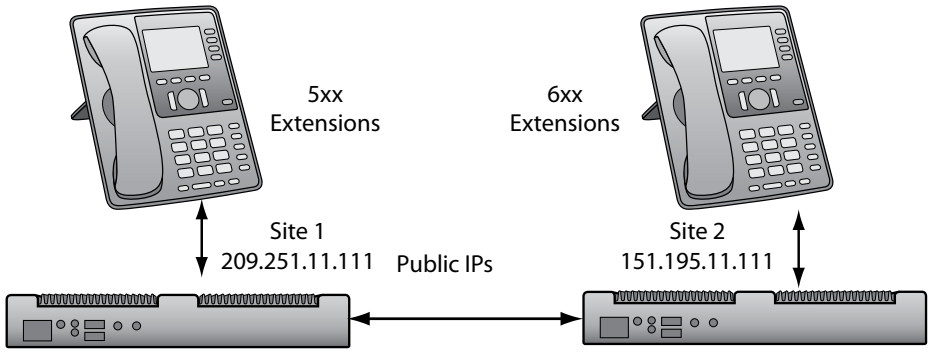


Figure 4-17. Connecting Branch Offices Using a Gateway Trunk

Create a trunk for each branch office, using the instructions that are shown below.

Branch Office 1

1. From the **Type** dropdown, select **SIP Gateway**.
2. Enter the IP address into the **Domain** field:

Name:	snomONE
Type:	SIP Gateway
Direction:	Inbound and outbound
Trunk Destination:	Generic SIP Server
State:	Enabled
Display Name:	
Account:	17772022934
Domain:	209.251.11.111
Username:	17772022934
Password:	••••••••••
Password (repeat):	••••••••••
Proxy Address:	alpha5.itsp.com

Branch Office 2

1. From the **Type** dropdown, select **SIP Gateway**.
2. Enter the IP address into the **Domain** and **Outbound Proxy** fields:

Name:	Pulsewan
Type:	SIP Gateway
Direction:	Inbound and outbound
Trunk Destination:	Generic SIP Server
Account:	
Domain:	151.196.11.111
Username:	
Password:	••••••••••
Password (repeat):	••••••••••
Proxy Address:	151.196.11.111
CO Lines:	

Using a SIP Registrations Trunk (SIP Tie Line)

The SIP registration trunk can be used to connect two branch offices when one of the offices has a private IP address. For example, a corporate head office has a pubic IP address, and a remote branch office has only one public IP address and requires that the system be on a private address but still wants to have connectivity back to corporate (Figure 4-18).

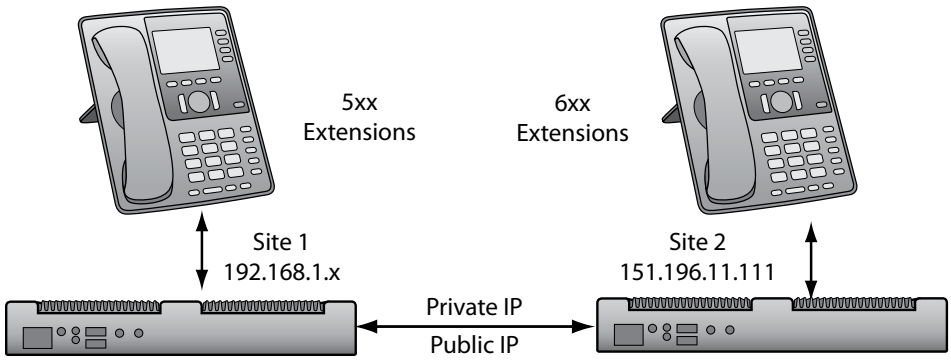
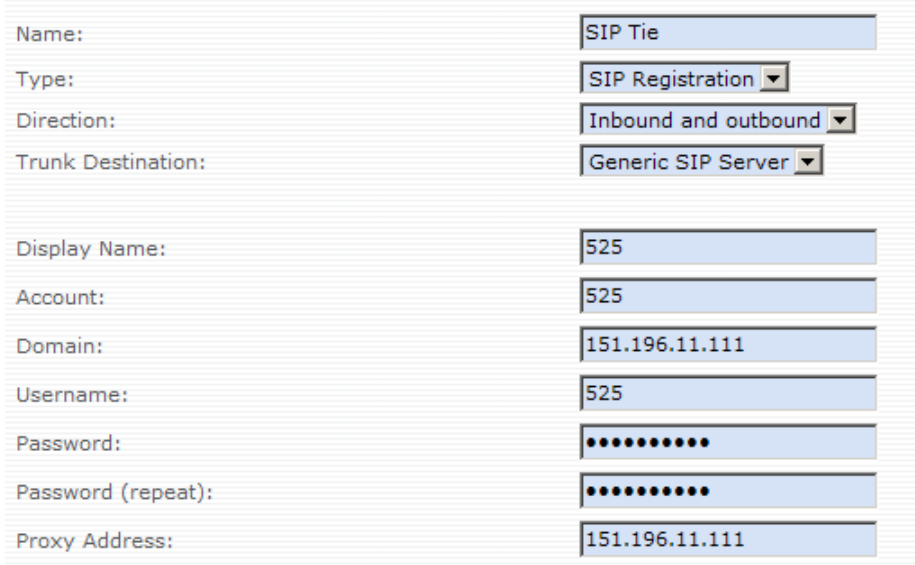


Figure 4-18. Connecting Branch Offices Using a SIP Tie Line

1. Create an extension that will be used by the trunk to route the calls:

2. Create a SIP registrations trunk for the branch office, entering the extension that will be used to route the calls (e.g., `525`).



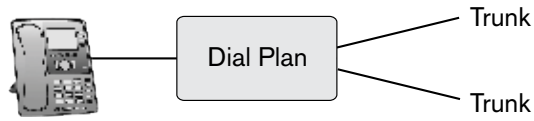
Once the offices have been connected, the headquarters will need to dial the extension that the trunk is routed to. Once the call hits the branch office, it will be sent to the auto attendant so that the headquarters can dial the remote extensions. The trunk has to register to the extension just as a phone would, so the system at the branch office

will need to register the trunk to the system at the headquarters, the same way an ITSP would need to be registered. Then anyone in the world can dial the DID, much like they would dial that extension.

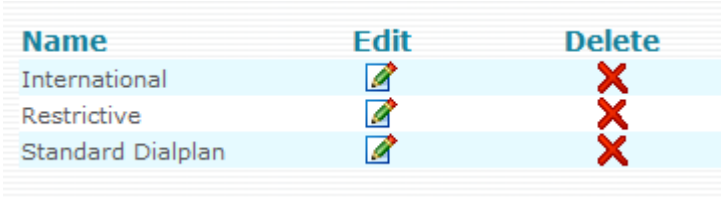
Chapter 5

DIAL PLANS

When an extension dials a number that is not available on the local snom ONE telephone system, the system must search for a trunk on which to route the call. To do this, it consults the dial plan. The job of the dial plan is to use pattern and replacement strings to route calls out different trunks. Since extensions map to dial plans, dial plans should be set up before extensions; however, if only one dial plan will be used and it will be the default dial plan, then this is not as important.



Multiple dial plans can exist on the same domain, but an extension can be mapped to only one dial plan. Administrators can assign the same dial plan to multiple extensions or create multiple dial plans and assign them to different users. A "restrictive" dial plan might be used to handle only local calls for phones in common areas, and an "international" dial plan might be used for international calling by executives.



Parts of a Dial Plan

Key Components

A dial plan consists of the following key components:

- **Preference:** The preference number is used to establish the preference order that will be used by the system when searching for a trunk on which to route a call. The system processes the available trunks beginning with the lowest preference value. (Identical preference values can be used for different trunks within the same dial plan; however, the system will randomly choose a trunk when more than one trunk meets the given criteria, so you should preference them.)
- **Trunk:** The trunk setting allows you to designate trunks that will be used by the dial plan. Trunks that are available for the domain are listed in the drop-down menu, and additional trunks can be added. Once trunks have been designated for a particular dial plan, the trunk that meets the pattern and replacement criteria for a particular call will be used to process the call.
- **C and P:** The **C** and **P** checkboxes determine how a call is handled once the user dials out onto the trunk. If the **C** checkbox is selected, the user will be prompted to enter a CMC code, but will not be required to. If the **P** checkbox is selected, the user will be required to enter a PIN number. This can be used to prevent unauthorized callers from making international calls. The **C and P** setting works in tandem with the **CMC authentication for outbound calls** domain setting (see page 97). The CMC code can also be set from the domain address book or the personal address book.
- **Pattern:** The pattern field is used to interpret digit sequences that will be used to decide on routing. In most cases, simplified expressions consisting of literals, prefixes, and fixed patterns will suffice.
  - Literals: If you want to match a specific number, just enter the exact number (e.g., `911`). The literal will be the first match in the expression.
  - Prefixes: Prefixes allow you to route numbers that begin with identical prefixes through the same trunk. For example, by specifying the common prefix `9011` in the pattern field, all international numbers will be

routed through the same trunk. To indicate that a prefix is being using, an asterisk must be entered after the prefix (e.g., `9011*`).

- Fixed patterns: If you use an `x` in a pattern, the system will treat it as a wildcard for 0-9. For example, `978xxxxxxx` will route all calls beginning with the area code 978 through the same trunk.

- **Replacement:** The replacement string is used to convert digit sequences into a dial string for outbound calling. It is used in the `To` header as well as in the Request-URI.
  - Simple patterns such as literals, prefixes, and fixed patterns do not require a replacement string; the system will automatically use `sip:\1@\r;user=phone` as the replacement. If you use a prefix in front of a star, the system will insert that prefix before the match. For example, `1*` will put a `1` in front of the match.

    Following are some sample patterns and replacement strings.

    Example 1
    Pattern: `91*`
    Replacement: `1*`
    Input: `919781234567@domain.com`
    Output: `19781234567@domain.com`

    Example 2
    Pattern: `978xxxxxxx`
    Replacement
    Input: `9781234567@domain.com`
    Output: `9781234567@domain.com`

    Example 3
    Pattern: `911/411`
    Replacement:
    Input: `911`
    Output: `911@domain.com`

    Example 4
    Pattern: `xxxxxxx`
    Replacement: `234xxxxxxx`
    Input: `1234567`
    Output: `2341234567@domain.com`

Following is a sample dial plan. The trunks are listed in the order in which the system will look at each trunk. The notes that follow the dial plan describe the effect of the pattern and replacement fields.

Pref	Trunk	C	P	Pattern	Replacement	See Note
100	Unassigned	☐	☐			
50	Not Allowed	☐	☐	1900*		A
60	GSM Gateway	☐	☐	9783741234	19783741234	B
65	ITSP1	☐	☐	9783741234	19783741234	C
70	ITSP1	☐	☐	1978*	1978*	D
75	Sangoma	☐	☐	1978*	1978*	E
80	GSM Gateway	☐	☐	1978*	1978*	F
90	Sangoma	☐	☑	011*	011*	G
95	ITSP2	☐	☐	1888*	1888*	H
100	ITSP3	☐	☐	*		I

Notes

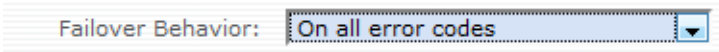
A. Not Allowed: This entry prevents anyone from calling 900 numbers.

B. Entries B and C are used to route calls that are forked to cell phone number `9783741234`. Whenever someone dials this number manually or if the system forks the call to the cell phone (or even if *00511 is dialed), then the system will try to route the call out the GSM gateway, then to the GSM phone. This method will prevent a hit on minutes.

C. See entry B above.

D. Entries D, E, and F: These entries are used in tandem to ensure that a call goes through even if you lose your Internet connection. The idea is if a call is sent to ITSP1 and it fails, it will be sent through the Sangoma trunk and if that fails because your internet is down, then the call will be sent out the GSM gateway.

Important: Failover behavior must be enabled on the trunk.



E. See entry D above.

F. See entry D above.

G. Sangoma: This entry is for international dialing. When this trunk is used, the user will be required to enter a PIN.

H. ITSP2: This entry is used for dialing 1888 calls.

I. All remaining calls will use this trunk.

Wildcard Patterns

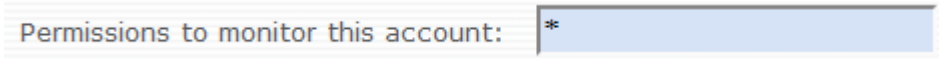
Wildcard patterns are a simple way to match a pattern in the system. This simple pattern-matching scheme, though not as powerful as the extended regular expression (ERE) pattern matching, can be used to solve most dialing issues. Table 5-1 lists typical usages of wildcard patterns.

Table 5-1. Wildcard Patterns and Usage

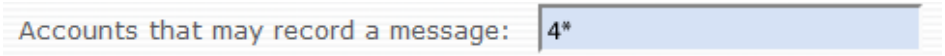
Wildcard	Definition
*	A star (*) matches any string of any length. *Note*: 9* matches anything starting with a 9 *but* *9 matches anything ending with a 9.
?	A ? matches any character and only one.
$	A $ matches a single number and only one.
%	A % matches any number (multiple digits or empty string).
[ ]	A range enclosed in brackets matches that range. *Note*: 11[02] matches the pattern 110 and 112.
\	A \ matches the character that follows.

Wildcard patterns can also be used in other places. To grant permission to all accounts, use a star (*). To limit the accounts, use a pattern such as 4* to allow all extensions that start with a 4. To grant permission to only one extension, place a single extension in the field.

- In the **Permissions to monitor this account** field: This field is included in all account types (extensions, auto attendants, hunt groups, paging accounts, service flags, etc.).

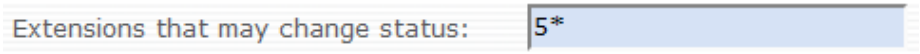


- In the **Accounts that may record a message** field: This field is included in agent groups, IVR nodes, and auto attendant accounts and is used to grant permission to record a greeting.



- In the **Source** field in Paging accounts: Use this field to specify which extensions can send a page.

- In the **Extensions that may change status** field: This field is used to change the status of a service flag.



Regular Expression Matching

The regular expression matching algorithm is a very flexible algorithm that follows the NAPTR algorithm of RFC 2915. For an exact description, please refer to this document (www.ietf.org).

The pattern string of the dial plan is surrounded by a `^` and a `$` to ensure that the whole string is matched. The system uses the username and the hostname. The port number, parameters, and the scheme are not included for the comparison.

If there is a match, the system will generate the resulting destination from the replacement string. The string may include references to matching groups in the pattern string. These matches are referred by the group number (starting with 1). Additionally, the matching string `r` may be used to insert the registrar name. For examples of algorithms, see “Examples of Dial Plans” on page 155.

Building a Dial Plan

Creating a Dial Plan

Every domain has its own dial plans, and any number of dial plans is allowed on a domain. The number of entries allowed on a dial plan is also unlimited.

1. To create a dial plan, click the **Dial Plans** tab.
2. Enter a name for the dial plan. The name can be any descriptive name. Spaces, numbers, and capital letters are permitted.

3. Click **Create**.

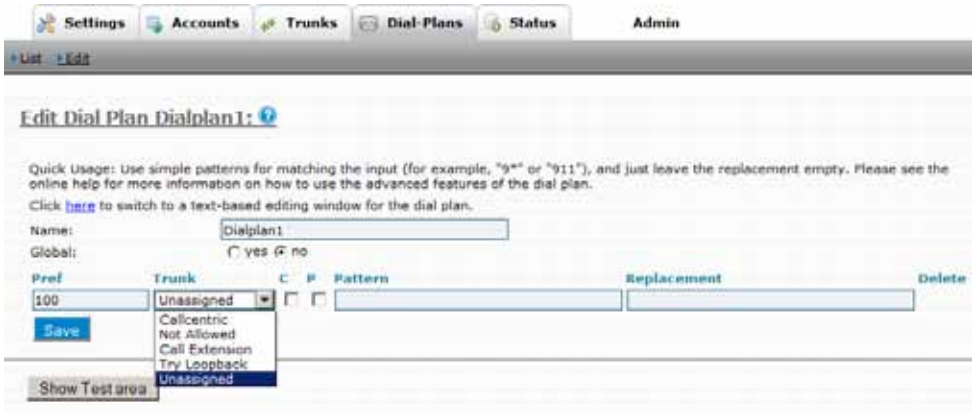
The dial plan has been created. Proceed to the next section to configure it. If you want to delete a dial plan, click **Delete** (be careful, as all dial plan data will be lost).

Configuring the Dial Plan

Once the dial plan has been created, trunks can be added. (Trunks must be created before they can be added to a dial plan. For more information on trunks, see Chapter 4.)

1. To add trunks to the dial plan, click **Edit** (as shown on the next page).

The following screen is displayed:



2. Set the **Global** setting. To make this dial plan accessible to all domains on the system, click **yes**.
3. From the **Trunk** dropdown list, choose a trunk. (Depending on the number of trunks that have been created for this domain, the dropdown list will vary.) In addition to trunks, other choices are shown below:
   - **Not Allowed:** This option is used to identify a pattern of numbers that should be denied by the system. When this mode is used, the system will stop processing the dial plan when that pattern is encountered. This makes it easier to define outgoing calls for which the called party is charged the cost of the calls by the telephone carrier, instead of the calling party (e.g., 900 numbers or expensive numbers like Afghanistan, which should never be called).

- **Call Extension:** This option is used to send a call to a registered extension. In this mode, the replacement field must contain an extension number. In most cases, you can just enter the extension (e.g., `123`). But you can also use the rules for generating a replacement pattern, including the `\1...\9` replacement strings. This is useful if you have a remote FXO or GSM gateway (which is behind a remote NAT device) that you want to route calls to. This allows you to take advantage of snom ONE and SBC.
- **Try Loopback:** This setting is not applicable to single-domain environments. In multi-domain environments, this mode is used to send a call from one domain to another domain (on the same system) without using an external SIP proxy. In this mode, the system will first check to see whether there is a match of the pattern and then calculate the destination using the replacement pattern. If the destination matches a telephone number (starting with "+") on the local system, then the PBX will send the call back to the system.

  Note: Before you can use the **Try Loopback** mode, you must disable the **Loopback detection** setting (see page 52), and you must have at least one UDP socket (not bound to any specific address or bound to the loopback address 127.0.0.1 or [::1]).

4. Enter a **preference** value for the trunk (default is 100).
5. Enter a **pattern** that the system will use when interpreting digit sequences.
6. Enter a **replacement** string that will be used to convert digit sequences into a dial string for outbound calling.
7. Click **Save**.
8. Repeat Steps 2 through 7 for each trunk that needs to be added to the dial plan.

Sample Dial Plans

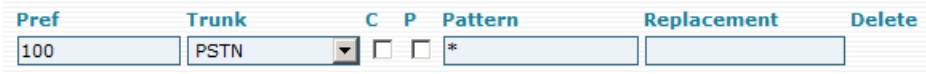
Typical Dial Plan

A typical dial plan would include the string `([0-9]*)@.*` as pattern and `sip:\1@\r;user=phone` as the replacement. The pattern string has one group `[0-9]*` (which is referred in the replacement string as `\1`). That means that if the pattern is matched against the value `2121234567@test.com`, it will store `2121234567` in the first

group and the result will be `sip:2121234567@test.com;user=phone` (the `user=phone` indicates to the recipient that the number is a telephone number).

A Simplified Dial Plan

In many cases, you may just want to route all numbers to an outside trunk. This can be done easily by using the pattern `*`. You don't need to fill anything into the replacement field (the system will do this automatically).

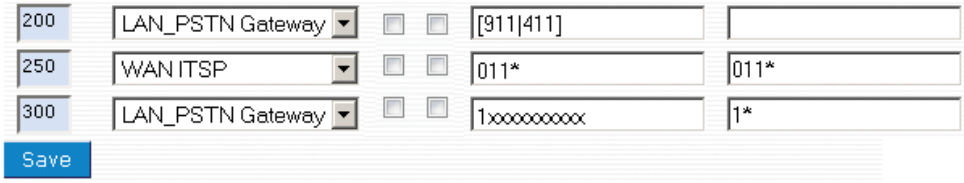


Dial Plan with Prefix in Front of the Number

If you use a pattern like `1*` in the replacement field, the system will automatically put a `1` in front of the match that it found in the pattern field. In the case when you use the pattern `9*` and dial the number `92121234567`, the system will automatically convert that into a `12121234567`.

A North American Dial Plan

If you use the snom ONE telephone system in the fixed-length dial plan of North America, you may use a dial plan similar to the one that follows:

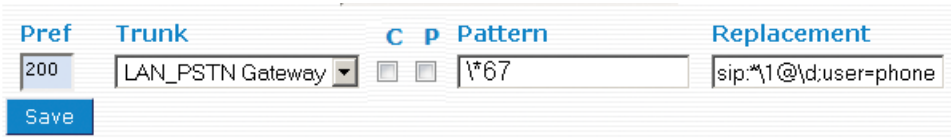


- `9[911|411]`—The first pattern matches the emergency number and the service number explicitly and sends it to the local gateway. It is a good idea to have an entry for these important numbers so that they don't accidentally get routed to the wrong gateway.
- `011*`— The second pattern matches all international numbers and sends them to a special trunk, which is intended to save costs for international calls.

- `1*`— The third pattern deals with all domestic calls. The fixed-length pattern was used so that the system can actually tell when this number is complete. You could add another pattern like `91978xxxxxxx` and send those calls to another trunk if you have negotiated a flat rate with your local PSTN service provider.

Sending Star Codes on a Trunk

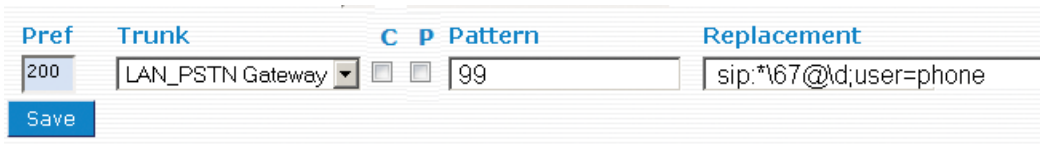
Extended regular expressions can also be used when sending star codes on a trunk.



When passing a star (*) to the carrier, a backslash is required before the star (e.g., `\*67`); otherwise, the system will treat the star and the numbers that follow as a star code. In the sample shown above, a backslash has been placed before the Block Caller-ID (*67) star code, so when the trunk is used, the system will replace the `\*67` with a `*67`, causing the caller-ID to be blocked. (The `d` in the latter part of the string tells the system to replace it with the domain. If an `r` had been used, the system would replace it with the registrar.)

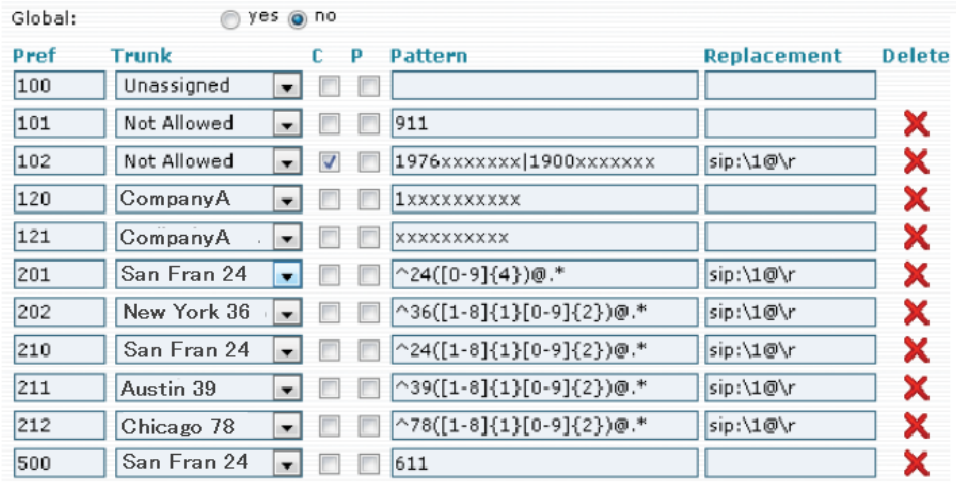
Important: When using star code patterns in dial plans, you must remove the code from the standard star codes and/or any customized codes.

If you'd rather not use star codes in the pattern field but still want to have the dial plan activate a star code, you can use a workaround. You can create a "stand-in" star code that will be used to correlate with the desired star code. In the example shown below, users will need to enter `99` before entering the actual phone number. The system will replace it with the *67 star code. This method allows you to retain the *67 star code as part of the default list of star codes; however, users will need to be informed ahead of time so they that will know to enter `99` before entering the phone number.



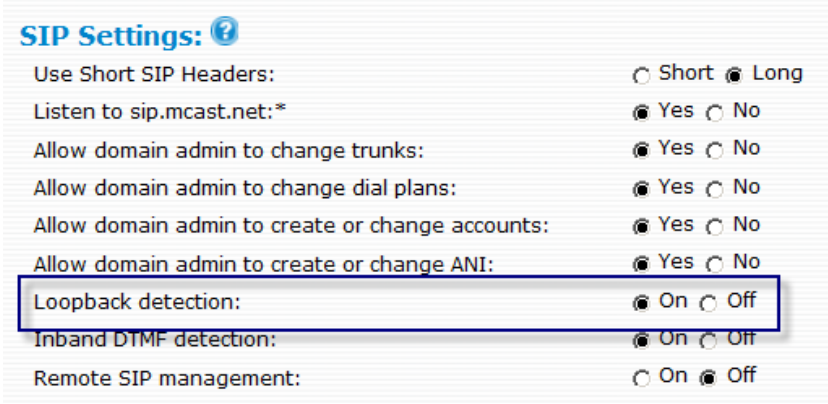
Forced Matching

The following dial plan illustrates the use of the caret. It's being used to force the system to begin matching from the start of user input.


Global: yes no
Pref Trunk C P Pattern Replacement Delete
100 Unassigned
101 Not Allowed 911
102 Not Allowed 1976xxxxxxx|1900xxxxxxx sip:\1@\r
120 CompanyA 1xxxxxxxxxx
121 CompanyA xxxxxxxxxx
201 San Fran 24 ^24([0-9]{4})@.* sip:\1@\r
202 New York 36 ^36([1-8]{1}[0-9]{2})@.* sip:\1@\r
210 San Fran 24 ^24([1-8]{1}[0-9]{2})@.* sip:\1@\r
211 Austin 39 ^39([1-8]{1}[0-9]{2})@.* sip:\1@\r
212 Chicago 78 ^78([1-8]{1}[0-9]{2})@.* sip:\1@\r
500 San Fran 24 611

Inter-Domain Dialing

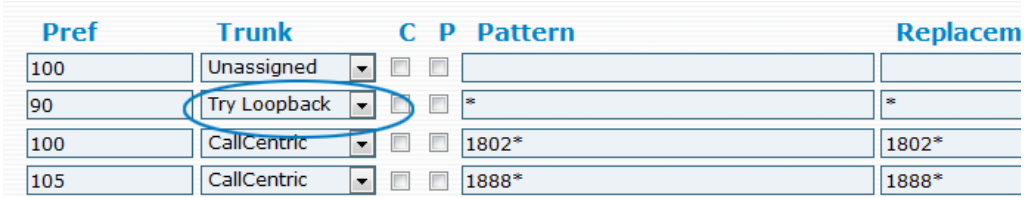
When configuring inter-domain dialing, activate the **Loopback detection** setting as shown below. Then proceed with your dial plan configurations as detailed on the next page.


SIP Settings:
Use Short SIP Headers: Short Long
Listen to sip.mcast.net:* Yes No
Allow domain admin to change trunks: Yes No
Allow domain admin to change dial plans: Yes No
Allow domain admin to create or change accounts: Yes No
Allow domain admin to create or change ANI: Yes No
Loopback detection: On Off
Inband DTMF detection: On Off
Remote SIP management: On Off

Domains with Non-Overlapping Extensions

If you have domains with non-overlapping extensions, use the following instructions to configure your inter-domain dialing. (DIDs, by nature, are non-overlapping.)

1. For each domain, create a dial plan entry with **Try Loopback** in the **Trunk** field.
2. Enter * for both pattern and replacement. If your DIDs aren't at least six digits long, add a prefix in the replacement field so that the system will convert them to six digits.



Note: Be sure to place the loopback dial plan entry at the top of the dial plan; however, 911, 411, 611, etc., can be the topmost entries.

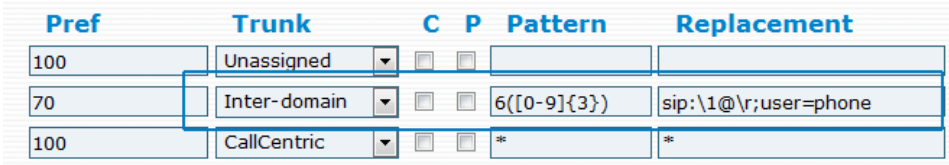
Domains with Overlapping Extensions

If the extensions between the different domains are overlapping, users will need to dial a prefix before the actual extension number is dialed. For this configuration, you will need to designate a prefix and provide proper pattern and replacement strings.

Note: Prefixing simply makes extension numbers non-overlapping; however, prefix-based dialing can be used for both overlapping and non-overlapping extensions.

1. From the first domain, create a gateway trunk that will be used to dial to the other domain(s).
2. Create a dial plan entry that uses the gateway trunk just created.
3. Choose a prefix. Be sure to choose a prefix that doesn't conflict with your other extensions (i.e., if the domain has extensions beginning with 5, you must use a number other than 5).
4. For the **Pattern** field, enter the prefix you've chosen followed by a string that corresponds with the number of digits your extensions have. The example

shown below is useful for three-digit extensions and will require users to dial a 6 before dialing the extension number (e.g., if the user dials 6400, extension 400 will be called).



5. For the **Replacement** field, enter `sip:\1@\r;user=phone`. (It is not necessary to specify the domain name here. The PBX will use whatever is configured on the trunk.)
6. Repeat these steps from the other domain(s).

Chapter 6

EXTENSIONS

Extensions are at the foundation of the IP telephone system and are essentially the phones that are registered to the system for making and receiving calls. Without extensions, the system would be of little use since there would be no one to call.

This chapter shows you how to create and configure extensions. Extensions have a wide selection of settings, and many of them can be set by the user. This chapter addresses only the settings that are necessary to get the extension ready for the user. These settings include the initial settings that are set when the extension is created, the registration settings, and the permission settings. Registration settings allow the administrator to define the maximum number of lines and concurrent registrations for the extension, and permission settings are used to grant access to advanced system functionality, such as Call Barge and Listen In. A handful of administrator settings can also be set from the user account, and they are discussed here. For information on the extension settings that can be configured by the user, see Chapter 22.

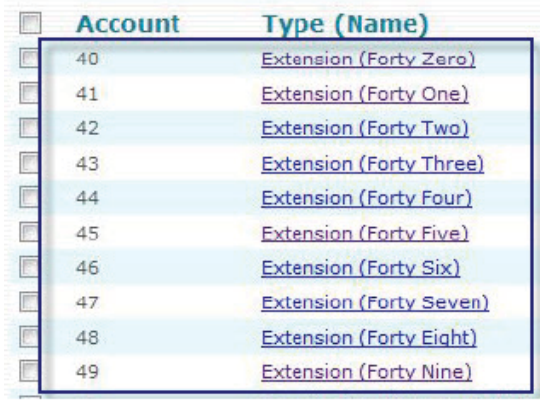


Figure 6-1. Extensions on the snom ONE Telephone System

Preparing the User Account

When preparing extensions for your users, you have a few options. You can use the default extensions that come with the system, or you can create new ones. This section guides you through both.

Working with Default Extensions

The snom ONE telephone system comes with ten preconfigured, two-digit extensions. To modify these extensions, use the following procedure:

1. Click the **Domains** tab.
2. Select the domain and click **Accounts**. The accounts list will be displayed as shown below:

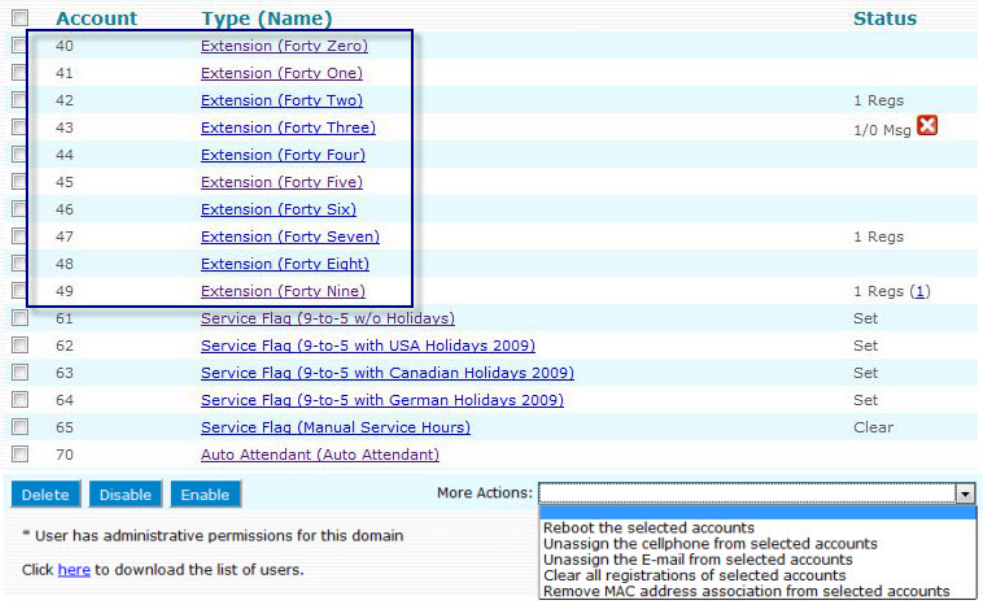
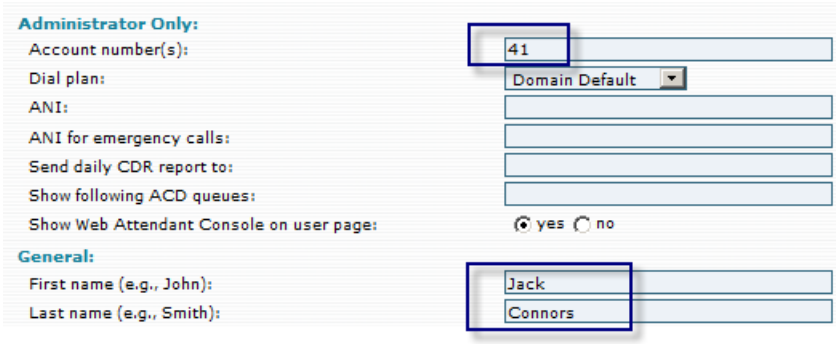
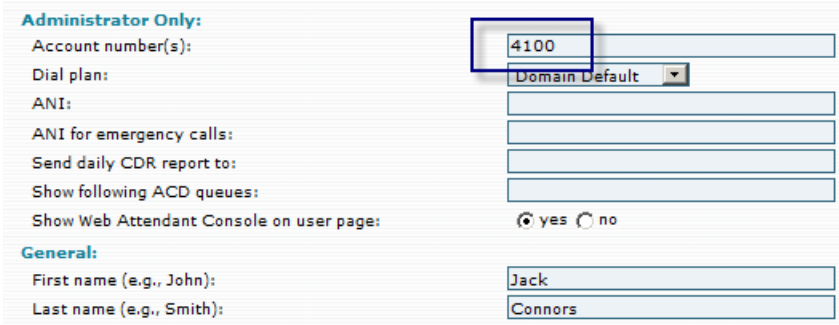

Account
Type (Name)
Status
40 Extension (Forty Zero)
41 Extension (Forty One)
42 Extension (Forty Two) 1 Regs
43 Extension (Forty Three) 1/0 Msg
44 Extension (Forty Four)
45 Extension (Forty Five)
46 Extension (Forty Six)
47 Extension (Forty Seven) 1 Regs
48 Extension (Forty Eight)
49 Extension (Forty Nine) 1 Regs (1)
61 Service Flag (9-to-5 w/o Holidays) Set
62 Service Flag (9-to-5 with USA Holidays 2009) Set
63 Service Flag (9-to-5 with Canadian Holidays 2009) Set
64 Service Flag (9-to-5 with German Holidays 2009) Set
65 Service Flag (Manual Service Hours) Clear
70 Auto Attendant (Auto Attendant)
Delete
Disable
Enable
More Actions:
Reboot the selected accounts
Unassign the cellphone from selected accounts
Unassign the E-mail from selected accounts
Clear all registrations of selected accounts
Remove MAC address association from selected accounts
* User has administrative permissions for this domain
Click here to download the list of users.

Figure 6-2. Default Accounts

3. Replace the **First name** and **Last name** fields with the user's name.



4. If you want to switch from 2-digit extensions to 3- or 4-digit extensions, you can do that here (e.g., change `41` to `4100`). Otherwise, go to the next step.



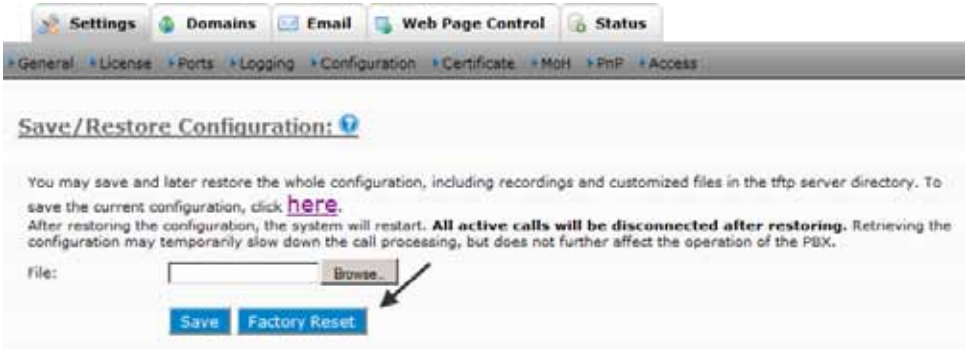
Note: After changing the number of digits of the extensions, the **PnP Dial-plan Scheme** setting will need to be reset so that the phone will allow the user to enter the necessary digits before it begins processing the call (this setting is detailed on page 107).

5. Set the general user settings detailed on page 166.
6. Click **Save**.
7. Before you register the account, configure the administrator, registration, and permission settings. The descriptions for these settings begin on page 167.

Importing Multiple Extensions (Bulk)

When a large number of extensions are involved, CSV files will expedite the process (see Appendix A for instructions on creating CSV files).

1. Reset the system to factory defaults by clicking **Admin** > **Settings** > **Configuration**.
2. Click **Factory Reset** as shown below:


Settings
Domains
Email
Web Page Control
Status
General
License
Ports
Logging
Configuration
Certificate
MoH
PnP
Access
Save/Restore Configuration:
You may save and later restore the whole configuration, including recordings and customized files in the tftp server directory. To save the current configuration, click here.
After restoring the configuration, the system will restart. All active calls will be disconnected after restoring. Retrieving the configuration may temporarily slow down the call processing, but does not further affect the operation of the PBX.
File:
Browse...
Save
Factory Reset

   This will clear the system of all default accounts and will allow you to start fresh.
3. Create the extensions using CSV files as detailed in Appendix A.
4. Once the accounts have been created, the administrator, registration, and permission settings need to be configured. The descriptions for these settings begin on page 167.

Creating a Few New Extensions

If you want to create new extensions and have only a few to create, you can create them manually. To create a few extensions, use to procedure below:

1. From the **Accounts** tab, click **Create**.

2. Select **Extensions** from the dropdown.

3. Populate the fields using the information shown below:

   - **Number**: This field takes an extension number and/or alias, i.e., a DID number. DID numbers allow users to be reached directly and are useful for phones that do not support 2, 3, or 4-digit dialing. An unlimited number of DIDs can be directly tied to an extension (DIDs can also be used without an extension account). When entering DIDs as aliases to an extension number, use the following syntax:

     `505/9781234567/9781234567`

     Note: If you use a space instead of a slash (`505 9781234567`), you will create two separate accounts that will be unrelated to each other.

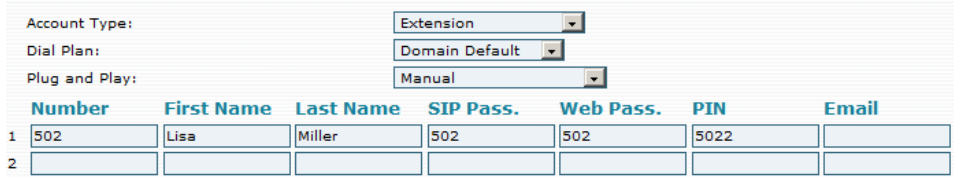
     Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts using the Accounts Page Display settings (see page 101).

     Note: Extension numbers should range from 2 to 4 digits. The number of digits must correspond to the **PnP Dialplan Scheme** setting so that the phone will allow the user to enter the required number of digits before it begins processing the call (see page 107 for more information on this setting).

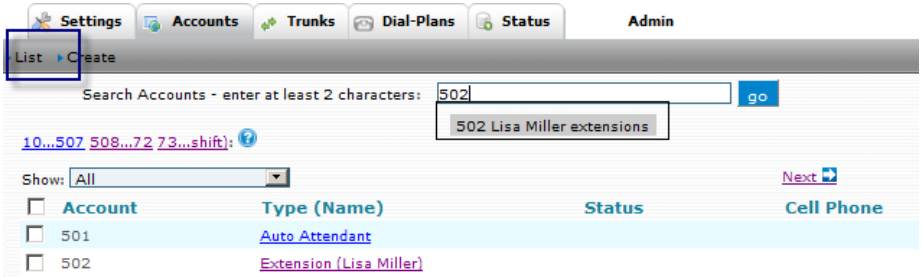
   - **First name:** The **First name** and **Last name** fields will be displayed for all internal and external calls (international characters are permitted). This is the case when calls are made from that extension or when the system sends email to its users.

   - **Last name:** User's last name.

- **SIP Password**: This password influences the connection between a user's VoIP phone and the system and influences a user's ability to access other registered SIP devices. When this password is set, the system will challenge SIP user agents on requests.
- **Web password:** The user will need this password when logging into the web interface and will be required to use a password that is based on the **Password Strength** setting set by the administrator.
- **PIN**: The PIN is used in several areas of the system (e.g., when a user accesses the voicemail system from another extension or from an outside line, when calling into the system from the cell phone, when using the calling card feature, and when hot desking). When you create extensions, you can leave the PIN field empty and opt to have users set up their own PINs. Once a PIN has been set up, no one other than a user who registers with the extension credentials will be able to go to the mailbox. For optimum security, we recommend at least five-digit PINs (see **Voicemail PIN Digits** on page 99).



4. Click **Create**.
5. To open the account, click **List** then click the account or use the search box at the top of the screen.



The following screen will be displayed:

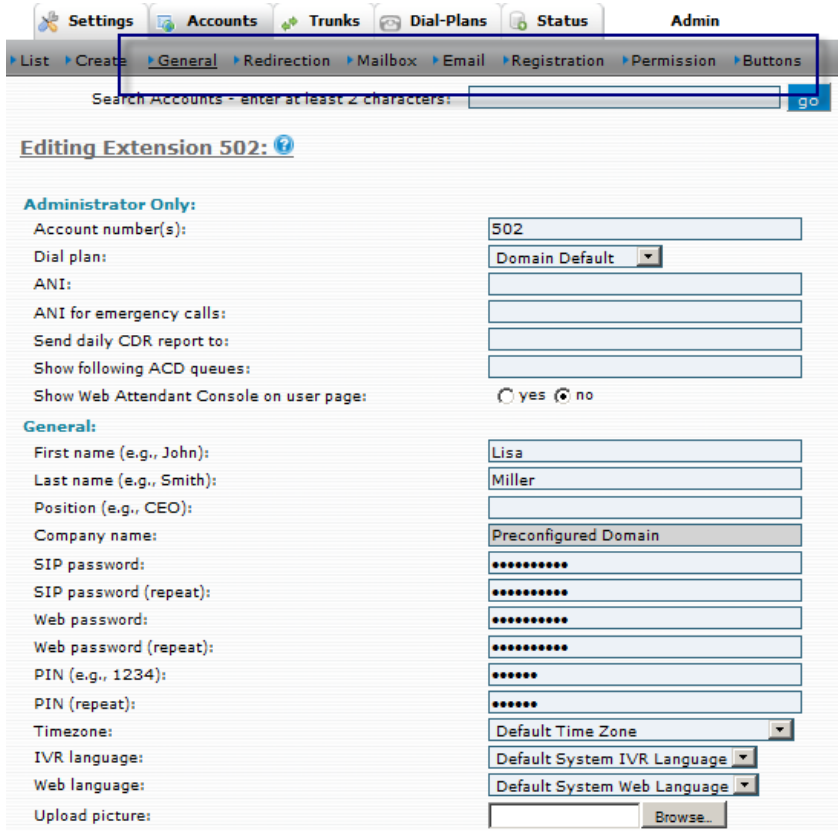


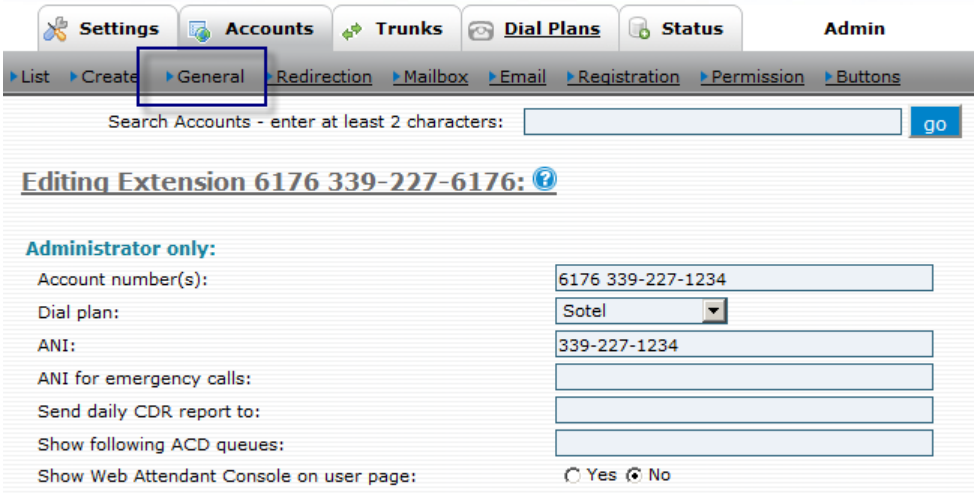
Figure 6-3. General User Settings (as seen by the admin)

Once the account has been created, the administrator, registration, and permission settings will need to be configured. These settings are outlined in the next section.

Before Registering the Extension

Administrator-Only Settings

Each extension has a set of administrator-only settings that are visible only to administrators. These settings are located in the **General** link in the user's account.



- **Dial plan:** Dial plans determine which trunks are used for outbound calls. Dial plans that are available on the domain will show up in this dial plan dropdown (see Chapter 5 for information on dial plans).
- **ANI:** ANI (Automatic Number Identification) is a service that tells the recipient of a telephone call which telephone number made the call. In most cases, the ANI is used in the `From` field in the SIP packets or the caller-ID. Each domain can be configured with a default ANI (page 95) or you can specify a unique ANI here.
- **ANI for emergency calls:** The system will send this ANI when the emergency number has been dialed.
- **Send daily CDR report to:** Enter the extension number(s) that should receive the CDR report for this extension. Use semicolons between multiple email addresses, since email addresses may contain spaces (e.g., Fred Feuerstein <ff@domain.com>; Carl Clements <cc@domain.com>). For detailed information about CDRs, see Chapter 22.
- **Show following ACD queues:** This setting is directly related to the **Queue Manager** setting that is part of the agent group account (page 236). A queue manager is a user who monitors agent groups.

- **Show Web Attendant Console on user page:** The Web Attendant Console (WAC) allows users to monitor extensions, join conferences, and do many system-related tasks.

Registration Settings

The **Registration** tab is used to control the registrations for the account. You may register one or more devices for one extension. When an extension is called, the system will call all registered extensions in parallel. The first extension that picks the call up will get the call, and the other extensions will receive a CANCEL message.

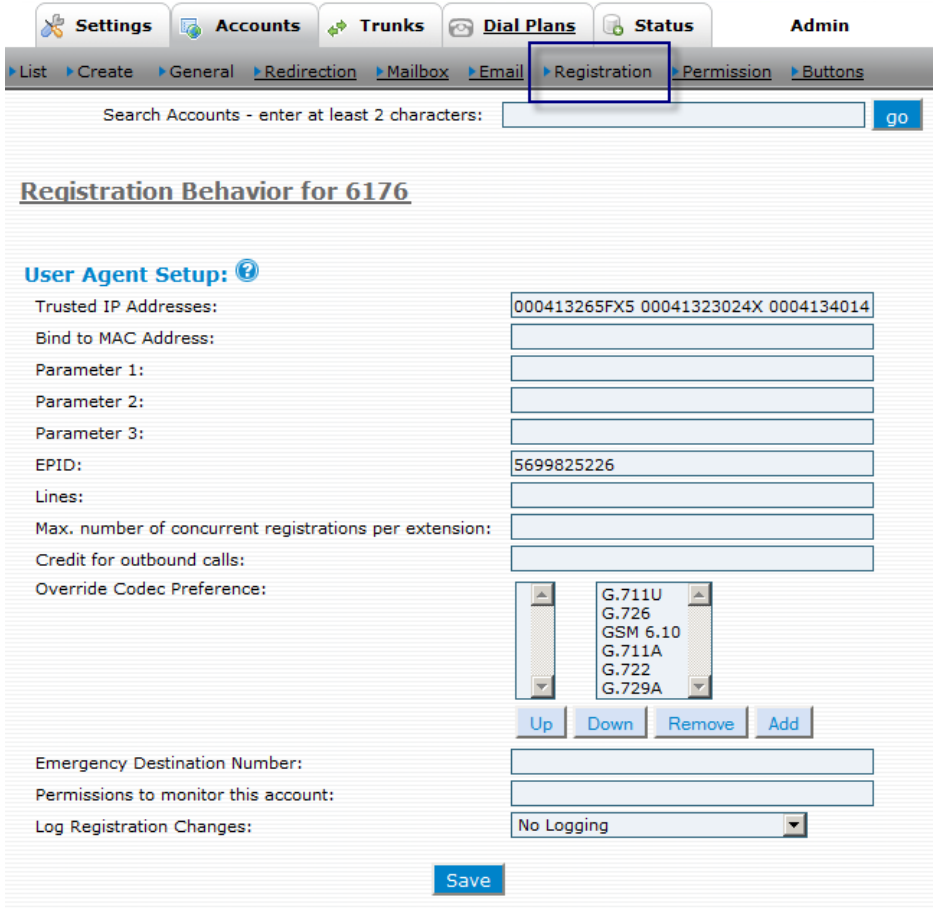
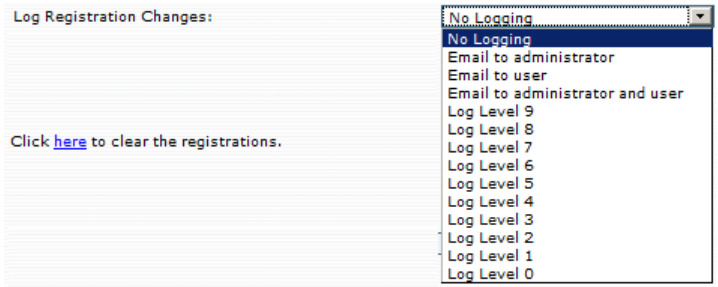


Figure 6-4. Registration Settings

Use the following information when configuring the resistration settings shown in Figure 6-4:

- **Trusted IP Addresses:** This setting dictates which IP address or addresses can be registered to this extension. The system will accept registrations only from the specified IP addresses. For example, if the extension has been set to `192.168.1.2` and `192.168.1.5` tries to register, it will be denied with a 403 forbidden message. Use a space as a separator when entering multiple IP addresses. To indicate subnets, use a slash and the number of significant bits behind it (e.g., `192.168.2.0/24`).
- **Bind to MAC Address:** This field is used to bind the registration to a specific user agent. To find the MAC address for a phone, press the "?" on the telephone keypad. The MAC address will appear in the telephone display.
- **Parameters 1 through 3:** Parameters 1 through 3 can be used in various places as generic, extension-related parameters. All parameters can be used to TAG extra fields onto the REPLACEMENT part of the dial plan, a way of passing information out of the system (in SIP) to another server. This is normally used for billing, e.g., `sip:*@\r;id1=\x;id2=\y;id3=\z`.
  - Parameter 1: If set, it will be used in as CLI if set on an outbound call.
  - Parameter 2: This field is a tagging field. Whatever is placed in this field will appear in the SOAP lookup mechanism.
  - Parameter 3:
- **EPID:** EndPoint Identifier is a random number created by the system. The EPID is sent on all 911 calls, enabling the PSAP to call the extension back directly if the phone is disconnected or the person hangs up. The EPID is essentially a DID for that extension and ensures that a returned call will reach the extension from which the call originated even if there is an auto attendant in the middle. This works to enable 911's E911 service.
- **Lines:** The lines parameter is used during provisioning to tell the phone how many line keys it should allocate (whenever applicable). The line feature is also used to restrict the number of calls that an extension can make. For example, if `1` is used in this field, then calls cannot be made simultaneously from both the office phone and the home office phone. During an active call, the system will neither page the extension nor perform intercom calls to that extension.

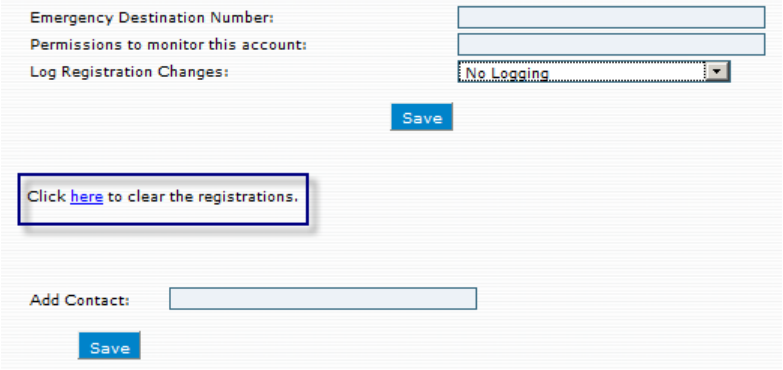
- **Max. number of concurrent registrations per extensions:** This setting is used to restricted the number of phones that can be registered to an extension. This is useful for service providers or enterprises that want to ensure only one phone is registered per extension.
- **Credit for outbound calls:** This setting allows you to place a limit on outbound calling for the extension only. You can also place a limit on outbound calling at the domain level (see **Credit for outbound calls** on page 98).
- **Override Codec Preference:** This setting allows you to specify the codec preference for the extension. This setting is useful for a remote phone with limited bandwidth, as you can force a low bit rate codec like GSM or G.729 to be used on the extension. The format for this setting is similar to the Port Setup section of the system.
- **Emergency Destination Number:** This setting is used when you are running the extension in a remote location where a different police department should be called. You will need to find the Public Safety Answering Point (PSAP) for this number; however, it is not a guarantee that a call will be routed there, so ensure that this is tested or approved if your carrier does not have 911 service.
- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this extension.
- **Log Registration Changes:** This setting allows the domain administrator to specify a log level for registration log messages specifically for the extension. This setting makes tracking down registration problems easier. You can also decide who should receive an email when the registration status does change—the administrator, the user, or both.



Current Registrations

Displayed at the bottom of the **Registrations** page are the current registrations (if any exist) for the account. Important information includes the type of registration, the registered contact address (as indicated in the registration message), and the length of time the contact has been registered. "REGISTER" in the Type field indicates a standard registration for receiving calls. Other registrations address specific event types, like message waiting indications.

Clearing registrations: To clear all registrations, use the link at the bottom the page. Be sure to refresh the registration from the user agent so that you are able to call it.



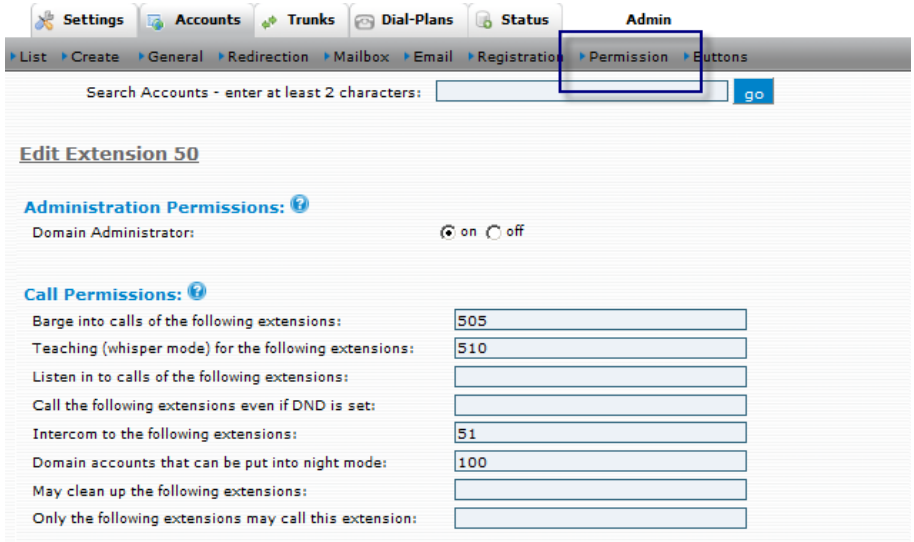
Sending a reboot request: You may also send a reboot request to the phone by clicking the **check sync** link. This way, you don't have to use the web interface of the device or even go to the phone to reboot it (for example, to read new configuration data).

Manual registrations: You can also add a registration manually. Manual registrations are useful for devices like Microsoft speech server that do not support registrations.

Static registrations: Static registrations can be used to call any other number.

Permission Settings

Permission settings allow administrators to define which features the extension can use. The permissions to jump into calls and listen to conversations may be legally restricted in certain countries, so use extra caution here. The permission to override DND is useful for assistant extensions that are responsible for screening calls.



Note: When entering extensions in this section, use a space as a separator if specifying multiple extensions. You may use wildcards, for example, an asterisk (*), to match all extensions of the domain.

Administration Permissions

- **Domain Administrator**: The permission to manage the domain should be given only to those who are allowed to change passwords, create or delete accounts, change dial plans and rates, and so forth.

Call Permissions

- **Barge into calls of the following extensions**: Call Barge-in allows a third party to barge into an in-process call. Typically, this third person is either a secretary contacting the boss or possibly a co-worker in the next cube who needs help on a call. The permissions to jump into calls and listen to conversations may be legally restricted in certain countries; please use extra caution here. Once permission has been set, Call Barge-in can be activated using the *81 star code (see page 445).
- **Teaching (whisper mode) for the following extensions**: Call Teach mode allows a third party on a line with only one of the parties knowing. This is typically useful in a call center when a trainer wants to offer tips to a new agent without the customer knowing. Once permission has been set, Call Teach can be activated using the *82 star code (see page 446).
- **Listen in on calls of the following extensions**: In Listen-In mode, a third party can listen in without being detected. The two parties speaking to each other are not aware of the listen-in. Users with permission to use Listen-in can activate it using the *83 star code (see page 446).
- **Call the following extensions even if DND is set**: If this flag is set, the account will be permitted to call the extension indicated in this field, even if that extension is currently on DND. This applies only to DND which has been set on the system. The permission to override DND is useful for extensions being used by assistants who are responsible for screening calls.
- **Intercom to the following extensions**: This feature is used for communicating with one other person. The two parties must each have their own extension number. (Intercom will not work between two phones that are registered to the same extension.) Users with permission to intercom can activate it using the *90 star code (see page 431).
- **Domain accounts that can be put into night mode**: This feature enables users to forward domain accounts (e.g., auto attendant, hunt group, etc.) to their own extension. Domain accounts that are entered into this field can be put into night mode by this user. Star code *80 is used to activate this feature (see page 443).

- **May clean up the following extensions**: This feature enables an extension to clean up other extensions and is useful in a hotel implementation where voicemail must be cleaned out and greetings reset. Star code *84 is used to activate this feature (see page 448).
- **Only the following extensions may call this extension:** This feature can be used to limit the users who can call another user's extension.

Chapter 7

PARK ORBITS

A park orbit is like a parking lot. It provides a holding place where calls can be parked while the callee is being located. Once calls have been parked on a park orbit, they can be retrieved by other users. Park orbits also provide an excellent solution to the dilemma users run into when trying to move a call from their corded IP phone to their cordless IP phone (e.g., from a snom 370 to a snom m9). Since the same extension is registered to both phones, calls cannot be transferred between them. Parking the call, then retrieving it from the other phone is a great workaround for this.

Park orbits are implemented through the Call Park (*85) and Call Park Retrieve (*86) features. Users must execute the *85 star code followed by the park orbit number to park calls on a park orbit. Other users can retrieve the calls by entering *86 and the account number of the park orbit. (A toggle button can also be set up to make it easier for the user to execute.)

Note: If a park orbit is not specified after *85, Call Park will fail. The call will not be parked on the user's extension as in the previous release.

Parking a call is different from putting a call on hold since it is designed to allow other extensions to pick up the call. With call hold, only the user who put the call on hold can pick it up.

Before users can execute the Call Park and Call Park Retrieve star codes, park orbit accounts must be set up.

Creating a Park Orbit

To create a park orbit:

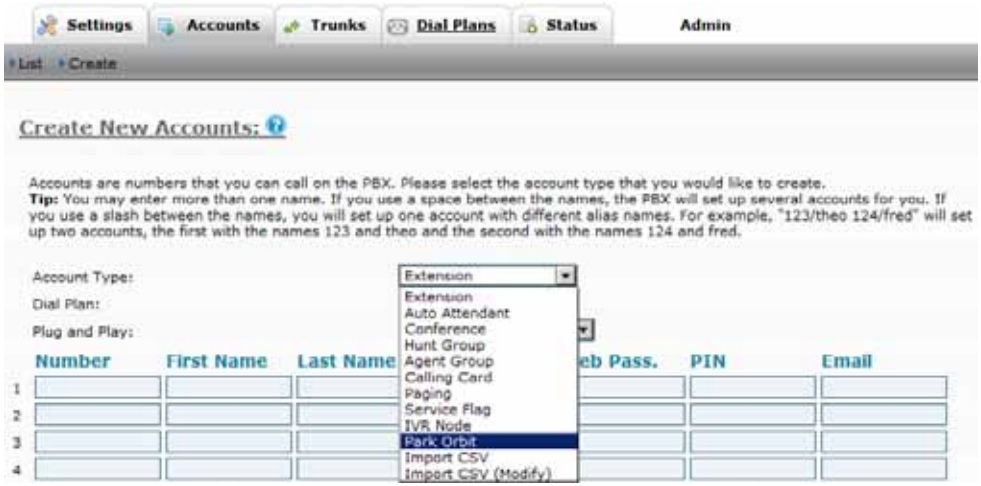
1. Click **Accounts** > **Create**.
2. Choose **Park Orbit** from the dropdown.
3. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

   `667/9781234567`

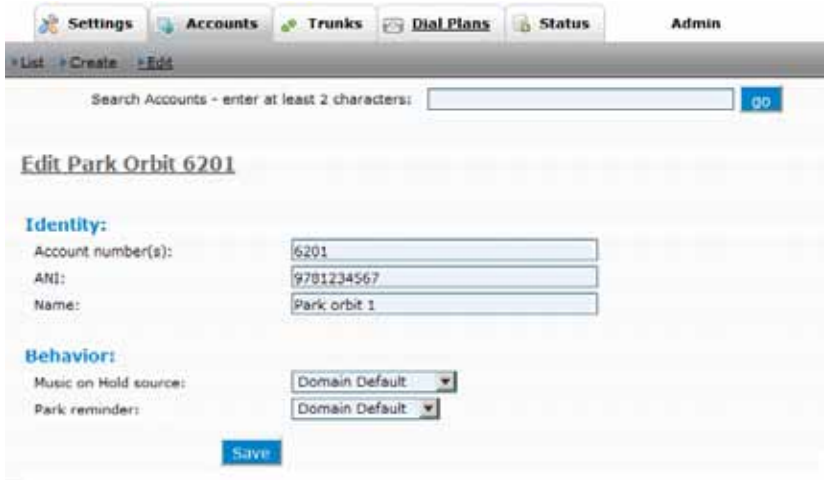
   Note: If you use a space instead of a slash (`667 9781234567`), you will create two separate accounts that will be unrelated to each other.

   Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts under the accounts page at the domain level (**Domain** > **Settings**).

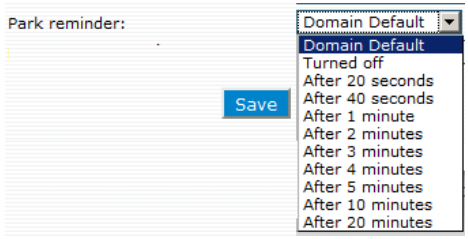
4. Click **Create**.



5. When the page reloads, click **List** to view the accounts, then click the account to open it.



- **Account number**: This field is automatically populated with the account information you entered into the **Account Name** field when the account was created.
- **ANI**: ANI (Automatic Number Identification) is a service that tells the recipient of a telephone call which telephone number made the call. In most cases, the ANI is used in the `From` field in the SIP packets or the caller-ID. Each domain can be configured with a default ANI (page 95) or you can specify a unique ANI here.
- **Name**: By naming the park orbit, you will be able to identify it more easily.
- **Music on Hold source**: From the dropdown, choose a music on hold source.
- **Park reminder**: Once a call has been parked and the required time has lapsed, the system will call back the extension that parked the call. This will serve as a reminder to the user that the caller is still waiting and that no one has picked up the call.



How the Park Orbit Works

Parking Calls

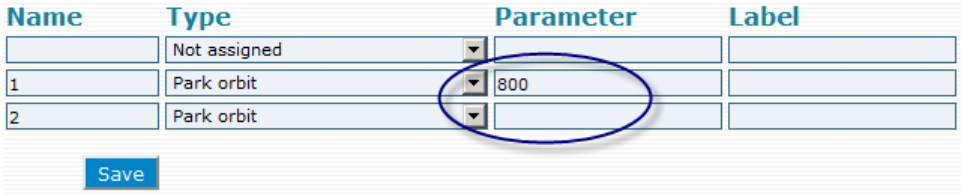
Once park orbits have been created, users must execute *85 and the park orbit number to park calls. Once *85 has been executed, the system will inform the user where the call is parked. This user can then track down someone who can retrieve the call (i.e., “Call on 800”).

Retrieving Calls

To retrieve a parked call, users must enter *86 followed by the park orbit number (e.g., *86800).

Using a Park Orbit Button

A **Park Orbit** button can be used to toggle back and forth between Call Park and Call Park Retrieve (see Chapter 19 for more information on setting up button profiles). A parameter is required with park orbit buttons (see image below). When no parameter is provided, the Call Park will fail.



Important: Before you can use this button, the star codes for Call Park and Call Park Retrieve must match (e.g., *85/*85). See Figure 23-1 on page 430.

Chapter 8

SERVICE FLAGS

Service flags give companies professional methods for handling callers who call after normal business hours. These options include (1) night service, which redirects callers to the extension or phone number of the person covering the business during closed hours, (2) voicemail, which allows the customer to leave a message and the company to respond as necessary, and (3) a recording of important information (e.g., hours of operation, directions, contact information).

A single service flag can be used for several accounts simultaneously, such as an auto attendant, an agent group, and a hunt group. Service flags can be controlled both automatically and manually and can be configured so that an LED on a user's phone will indicate whether the service flag is active or not. Other service flag features are listed in Table 8-1

Table 8-1. Service Flag Features

Feature	Functionality	Benefit
Automatic or manual	Service flags can be operated either automatically or manually. When service flags are used manually, users must press a button or dial the service flag account number to activate or deactivate it.	Automatic mode allows businesses with consistent closing hours to have the service flag activate on its own. Manual mode is useful for businesses with irregular closing times and for those who want to control it at a moment's notice.

Feature	Functionality	Benefit
Hunt group and agent group control	Several hunt groups can be used for different situations (normal operation, extra busy day, short-handed staff day), and their activation can be controlled with manual service flags.	Quickly shift between plans to reallocate calls, services, and staff. Advanced planning allows you to prepare for the call load.
Auto attendant control	Auto attendants are used to answer incoming calls and direct them to other destinations. Service flags let you control the greeting that is used and where the calls are directed.	Use several auto attendants to reduce the risk of losing business. Create one for day, lunch, and night (or prepare one in advance for unexpected closures) and switch as needed. Turn them off/on from a remote location by phone or via the Internet.
Controlled access to flags	Users can switch the service flag on and off.	Service flag control can be limited to managers at any on-site or remote location.
Simultaneous multi-account activation	The same service flag can be used for multiple accounts (e.g., hunt group, agent group, and auto attendant). All accounts using the flag will switch on or off simultaneously.	Prepare several complete business communication scenarios, and switch to any one of them quickly.
Visual indication	When a service flag has been turned on or off, the system sends a message to selected phones. When the service flag has been activated, a designated LED on phones that are configured to receive this indication will light.	Viewing the service flag activity can be limited to managers at any on-site or remote location.

Feature	Functionality	Benefit
Cell phone control	Cell phones can be linked to service flags. If an extension has subscribed to a service flag, then any calls made to that extension will be sent to the user's cell phone when that service flag is on.	After-hours calls can be sent to a manager's cell phone automatically. By using multiple after-hours service flags, calls can be sent to the appropriate manager on different days of the week.

Setting up a Service Flag Account

This section provides instructions for creating and configuring a service flag account:

1. From the **Accounts** tab, click **Create** and select **Service Flag** from the drop-down:

2. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

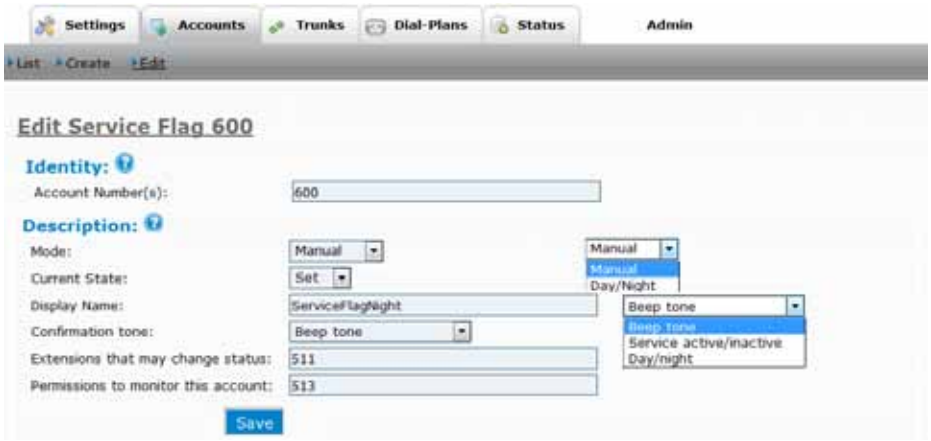
```
505/9781234567
```

   Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this happens, you can **hide aliased accounts under accounts page** at the domain level (**Domain** > **Settings**).

   To create multiple accounts at the same time, use a space between the numbers:

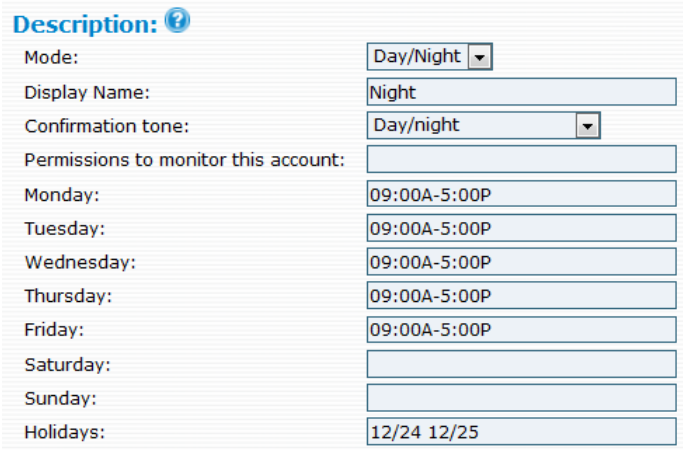
```
505 506 507
```

3. Click **Create**. When the page reloads, click **List** and open the account.



4. Use the following information to complete the service flag configuration:

   - **Account Number:** This field takes an extension number and/or DID number(s). The number of DIDs is unlimited.
   - **Mode**: The service flag can be controlled either manually or automatically. Choose a mode:
     - **Manual**: A manual service flag must be activated/deactivated manually (see "Setting/Clearing a Service Flag" on page 190).
     - **Day/Night**: A day/night service flag is controlled automatically according to a schedule you create. Following is a sample schedule:



When creating a schedule for a day/night service flag, refer to Table 8-2.

- **Display Name:** This setting allows you to enter a small description of the service flag to distinguish it from other service flags:

- **Current State**: This setting is reserved for the manual mode only. Choose **Set** to activate the service flag and **Clear** to deactivate it.
- **Confirmation Tone**: Choose the confirmation sound you would like to hear upon turning the service flag on or off.
  - Beep tone: The system will play a short beep to indicate that the service flag has been set or cleared.
  - Service active/inactive
  - Day/night
- **Extensions that may change status**: Enter the extensions that are permitted to change the service flag. An asterisk indicates that all users are permitted to change the status.
- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor the service flag.

Table 8-2. Day/Night Service Flag Requirements

Topic	Description
Format	You can use either of the following formats; however, both formats require start and end times (e.g., HH:MM-HH:MM): ▪ 24-hour format (e.g., 21:00 for 9:00 p.m.) ▪ English AM/PM style (e.g., 9:00P for 9:00 p.m.)
Multiple time segments	To specify more than one time segment, use a space between the two segments: ▪ 9:00-12:00 1:00P-7:00P

Topic	Description
Holidays	To specify the days on which you do not want the schedule to be activated, such as a holiday or any other day, use the holiday field: ▪ To specify one day, use the MM/DD format (e.g., 11/24 for November 24). ▪ To specify two days, use the MM/DD format with a space between the days (e.g., 12/24 12/25 for December 24 and 25).
Noon time	To specify time during the noon hour (between 12:00 and 1:00 p.m.), you can use 12:00, 12:00P, or 12:00PM. All are treated as day time 12 o'clock.
Midnight	To specify midnight, use either 00:00 or 24:00, depending on the start and end times. ▪ To *start* a time period at midnight, use 00:00 (e.g., 00:00-08:00). ▪ To *end* the time at midnight, use 24:00 (16:00-24:00).

Important: The day/night service flag will be active during the time *outside* the hours that are set in the service flag. For example, if the service flag is set to 09:00A-5:00P, the status of the service flag will show **Set** for all times after 5:00 p.m. and before 9:00 a.m. If night service is being used, calls will be routed to the indicated extension.

Linking a Service Flag to an Account

Once you have created a service flag, it must be linked to an account before the system will use it. This can be done using two methods: night service or message only (which can also be configured to allow the caller to leave a voicemail).

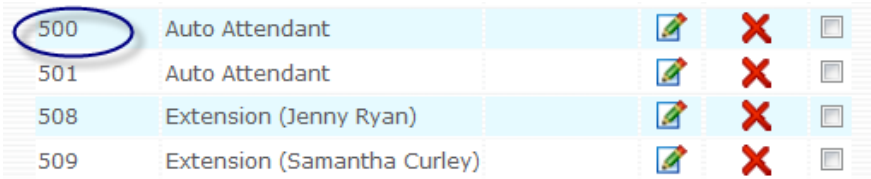
Method 1: Night Service

The **Night Service** setting allows you to provide service to callers during after-hours. Callers will be forwarded to the new number based on the service flag schedule.

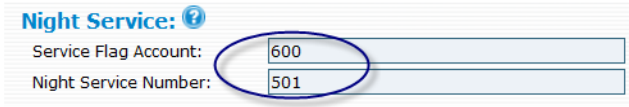
In our example, when service flag 600 is active, auto attendant 500 (an auto attendant with a day message) will forward calls to extension 501.

1. Create a day **Auto Attendant** (see Chapter 9).
2. Create a day greeting for the day auto attendant:

3. Open the auto attendant account.



4. In the **Service Flag Account** field, specify the name of the service flag that will be used (see below).
5. In the **Night Service Number** field, specify the account where calls will be directed (see below).



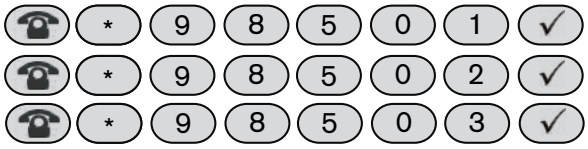
6. Click **Save**.

When the service flag is active, all calls will be forwarded to extension 501.

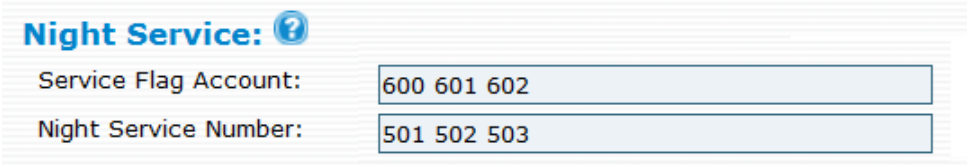
Multiple Night Service Numbers

You can use service flags to forward callers to multiple destinations depending on the time of day (i.e., a different destinations for different shifts):

1. Create a day auto attendant.
2. Create the necessary service flags.
3. Create the night service accounts (these can be auto attendants or extensions).
4. Create a greeting for each account being used as night service:



5. From the day auto attendant account, link the service flags to the other accounts.

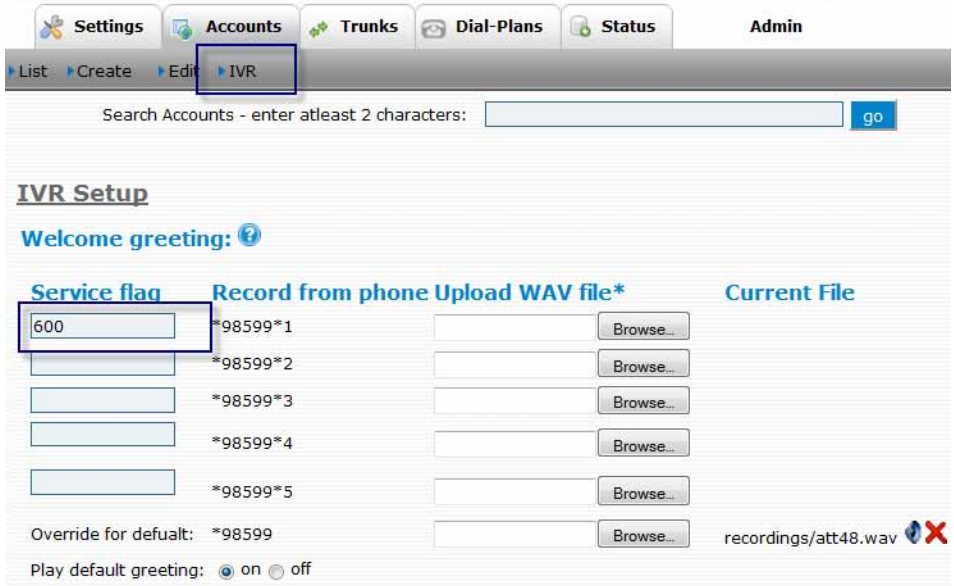


Method 2: Message-Only and Voicemail Options

If you don't want to provide service to callers during after-hours, use the **IVR** link from the auto attendant account. From this link, you can provide callers with a single message (e.g., "The office is closed, etc.") or provide them with numerous options: the option of dialing another extension, the option of leaving a voicemail, or the option of remaining on the line for general assistance.

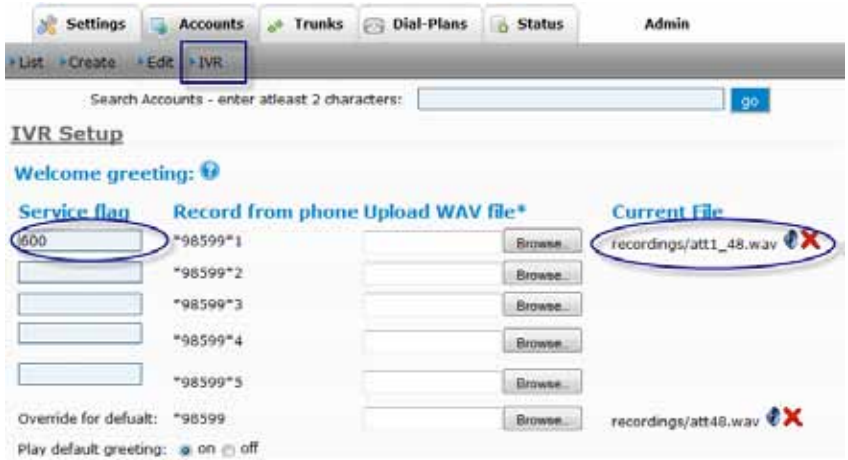
1. Create a day auto attendant.
2. Create a day greeting by entering `*98` and the account number (e.g.,`*98599`).
3. Create a night service flag and a schedule for the system to follow.

   Important: When listing the time schedule in a night service flag, be sure to specify the hours that your business is *opened*, as opposed to closed. Service flags become activated during the hours *outside* your listed schedule, so if the service flag is set to 09:00A-5:00P, the service flag will become activated anytime after 5:00 p.m. and before 9:00 a.m.
4. Open the auto attendant account.
5. Click **IVR**, as shown below.
6. Enter the service flag into the **Service flag** fields, as shown below.

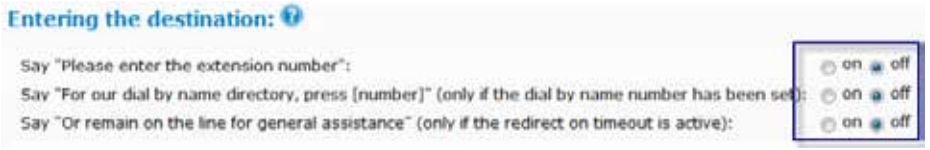


7. From the auto attendant, record a greeting for the night service flag. (In the example shown below, the auto attendant account is 599.)

The audio files will be listed under **Current File**:



8. To give the caller additional choices, choose from the options below:


Entering the destination:
Say "Please enter the extension number":
Say "For our dial by name directory, press [number]" (only if the dial by name number has been set):
Say "Or remain on the line for general assistance" (only if the redirect on timeout is active):
on off
on off
on off

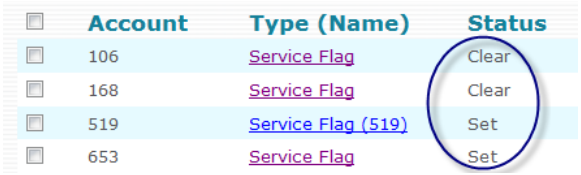
(For the last two options, see “Dial by Name” on page 205 and “Timeout Handling” on page 203.)

9. Click **Save**.

Note: If you need to change the message multiple times throughout the day (e.g., during lunch and after-hours), create a service flag for each period.

Setting/Clearing a Service Flag

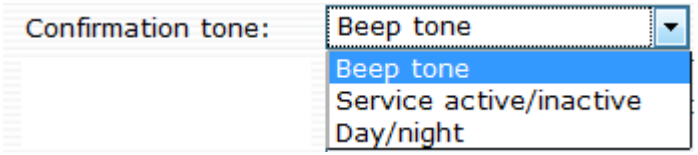
The **Set/Clear** status of a service flag can be seen from the **Accounts** tab:



Automatic service flags will become activated according to a schedule that you create. Manual service flags, on the other hand, need to be manually activated using one of the following methods.

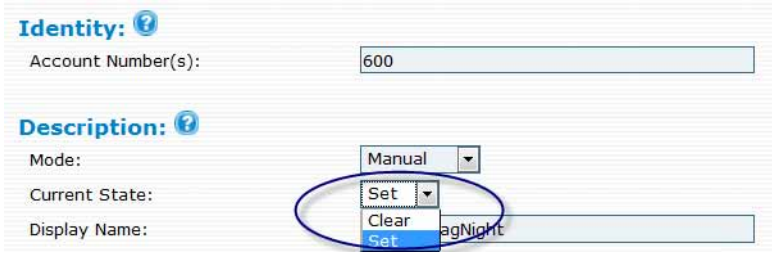
Setting a Manual Service Flag from the Phone

Call the service flag extension each time you want to change its state. The confirmation tone that is played is based on the **Confirmation tone** setting:



Setting a Manual Service Flag from the Web Interface

A manual service flag can also be set by using the **Current State** setting in the service flag account. This setting can be toggled between **Set** and **Clear**.

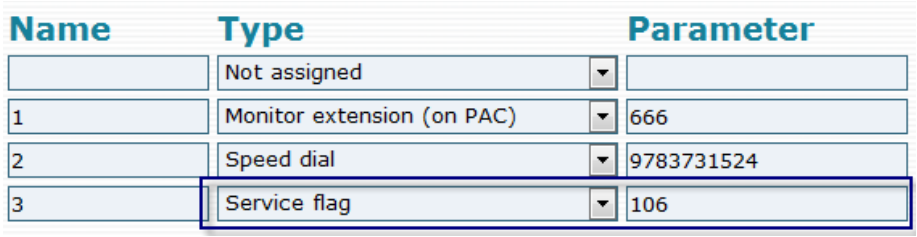


Service Flags and Buttons

Using a Button to Activate a Service Flag

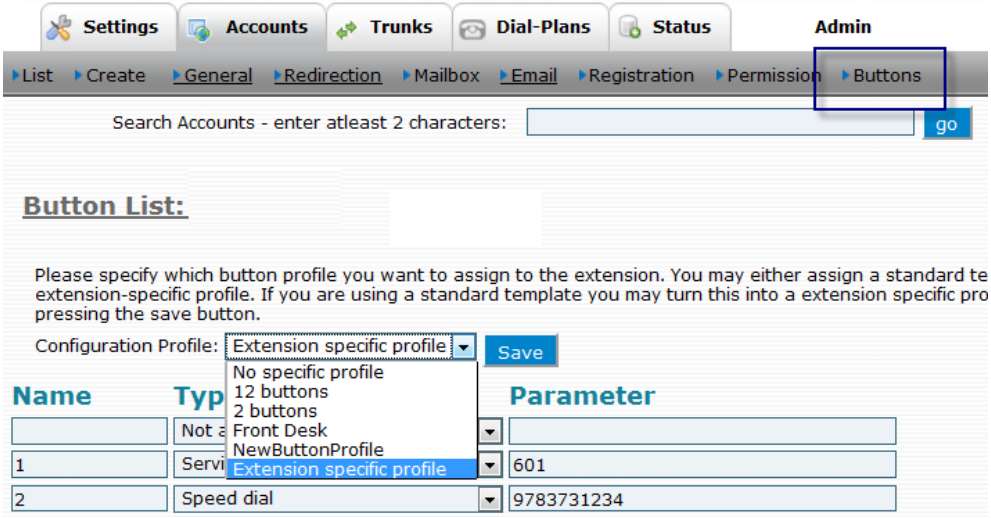
To activate/deactivate a service flag using a button, add a service flag button to the button profile of the extension that will be using it. (The instructions below assume you are adding the button from **Domain** > **Settings** > **Button**; however, it can be done from the extension itself.)

1. Open a button profile (or create one).
2. In the **Name** field, name the button (use a numerical value).
3. From the **Type** dropdown, choose **Service flag**.
4. Enter the service flag account number into the **Parameter** field.



5. Save the profile.

6. Open the extension that will be in charge of activating/deactivating the service flag.
7. Click **Buttons**.
8. From the **Configuration Profile** dropdown, assign the profile to the extension.



9. From the phone, press the button configured as **Service flag**. It will toggle between **Set** and **Clear**. The values assigned to the buttons correspond with the locations shown below:

Chapter 9

AUTO ATTENDANT

The auto attendant functions like a virtual receptionist, connecting incoming calls to extensions and other devices that have been configured to the system. The auto attendant often announces a company's name, followed by a selection of dialing options. A typical welcome message might be "Thank you for calling Company ABC, "for Sales, press 1," "for Accounts, press 2," and "for the dial-by-name directory, press 4." Callers press the number that corresponds with their selection and are directed accordingly.

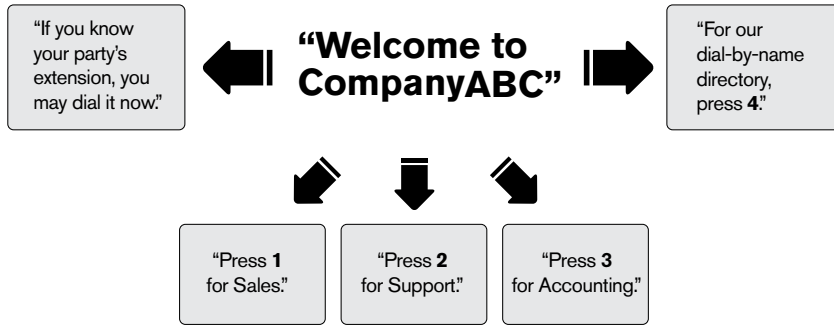

"If you know your party's extension, you may dial it now."
"Welcome to CompanyABC"
"For our dial-by-name directory, press 4."
"Press 1 for Sales."
"Press 2 for Support."
"Press 3 for Accounting."

Figure 9-1. Auto Attendant Welcome Message

Tasks performed by the auto attendant include searching for names, entering extension numbers, protecting certain extensions (e.g., phones that are on DND), and redirecting calls to external numbers. The auto attendant also performs other less visible tasks like calling back when an extension becomes available or redirecting calls into the mailbox.

The auto attendant can be configured to play time-dependent messages so that callers can be informed about a company's hours, and it can be configured to redirect calls to other extensions after normal business hours. This is known as night service and is configured through service flags.

Table 9-1. Auto Attendant Features

Feature	Functionality	Benefit
Dial-by-name service	The dial-by-name feature helps callers reach the correct person when they don't know the extension of the party they are trying to reach. Callers can enter the first or last name of person, and the auto attendant will play back the names that match the entry. Once the caller has made a choice, the auto attendant will connect the call.	The auto attendant can send a caller to an extension, a conference room, or a cell phone. This improves the caller's experience.
Non-reachable extensions	The auto attendant can be programmed with a list of extensions that callers will be unable to reach.	Call flow can be controlled for executives and others needing this service.
Transfer to cell phone	By setting an extension's mailbox escape account to an auto attendant, callers will be able to access that extension's Personal Virtual Assistant, which can be configured to provide the caller with the option of being transferred to that user's cell phone.	Callers can be provided with additional options, such as directions and latest news.
Selectable greetings	The auto attendant can be configured to play different greetings at various times of day. This feature allows you to have a different morning, lunch, after-hours, weekend, and holiday greetings.	A company can present a better image.
Nested auto attendants	An auto attendant can be created within another auto attendant.	Nested auto attendants allow callers to get closer to their desired destination.

Feature	Functionality	Benefit
Camp On and callback	Callers with a valid caller-ID can "camp on" a busy extension and receive a callback once the extension becomes available. (The system tracks a person's availability by monitoring keypad activity.) **Offer Camp On** must be enabled from the domain settings (see page 100).	The caller is given a choice when an extension they are trying to reach is busy, and communication is expedited.
Cell phone recognition	Callers who call into the auto attendant from a cell phone that has been configured to their extension are recognized by the system and can access the Personal Virtual Assistant.	Users can access star codes when away from their extension phone.
Blacklist control	Callers on an extension's blacklist are required to identify themselves before being transferred by the auto attendant.	Workers are not disturbed by unwanted callers.
Direct or WAV greetings	Auto attendant greetings can be recorded directly into the system from selected phones. Greetings can also be recorded by a professional recording studio and uploaded into the system via the Internet.	Professional greetings give a company a positive image.
Fax detection	The auto attendant can be configured to listen for a fax calling tone (the CNG tone). Upon detecting the tone, the system will transfer the call to its destination.	You can publish your main telephone number as your fax number (a separate telephone line is not necessary).

How an Auto Attendant Works

This section details the events that occur from the time the caller first reaches the auto attendant until the caller is connected.

Welcome Message

When someone calls into the auto attendant, the auto attendant plays a welcome message. The welcome message can be a standard message or one that varies according to time of day or week (see "Multiple Messages—Time-Based Configuration" on page 198). The caller can press the star key to skip the welcome message and go directly to the menu where the auto attendant asks for the destination, or the caller can listen to the available options (see Figure 9-1).

Processing User Input

Once the user has made a selection, the system must process the selection. Depending on whether the user entered numbers or letters, the process varies.

Numerical Input

In the simplest case, the system collects the digits for an extension and calls that extension, but the system also checks for direct destinations that might be associated with the input. Direct destinations are pre-configured destination fields that can be used to direct inbound calls to popular destinations like sales, support, and accounting (direct destinations are discussed on page 205). When an extension overlaps with a direct destination, the system calls the direct destination unless the auto attendant has been configured with a timeout. A timeout gives the system enough time to assess the user's complete input before connecting the call. For example, if a user enters 155 for an extension, but the system is using a "1" as a direct destination to Sales, the caller will be connected to Sales unless a timeout is in place. Figure 9-2 shows how user input is processed (based on an auto attendant similar to that shown in Figure 9-1).

Input	Processing Result
1 5 5	Caller is connected to Sales (if no timeout is in place).
4 5 5	Caller is connected to extension 455.
2	Caller is connected to Support.

Figure 9-2. Processing Numerical and Dial-by-Name Input

Dial-by-Name Input

When a caller uses the dial-by-name directory and has entered enough digits, the auto attendant searches through a name-searching directory. The digits correspond to the letters that are printed on the keypad button (2 = ABC, 3 = DEF, etc.). Key "0" maps only to the symbol "0," and key "1" maps to all other characters. In cases when the result is not unique, the auto attendant recites a list of matching names. When the user does not press anything, the auto attendant redirects the call to another destination.

Ringing an Extension

Once the auto attendant has processed the user's input, the auto attendant calls the extension. If the extension is not available and the user has only one line (see user's **Registrations** tab), the caller will be sent directly to the extension's voicemail. If more than one line has been designated to the extension, the caller will hear ringback and the user will hear a beeping noise (call waiting). If the extension does not pick up within the specified timeout, the caller will be sent to voicemail.

If the extension has specified a cell phone number and the time of day permits the inclusion of the cell phone, the auto attendant will include the cell phone in its list of ringing devices. This step may be delayed for a few seconds, allowing a user who is near the desktop phone the chance to pick up the call from that phone first. The ringback tone from the cell phone is ignored, preventing the caller from knowing where the call is picked up. While the extension is ringing, the caller can press the star key to cancel the call and enter a new number.

When the Extension Does Not Pick Up

If a user has programmed a redirection from an extension and does not pick up the call from that phone, the auto attendant will handle the call in one of two ways:

- If the call comes from an outside user, the caller will be sent to the extension's voicemail after the mailbox timeout has lapsed.
- If the call comes from either another extension or from a cell phone that is configured to an extension, the user can either camp on the extension or leave a mailbox message.

If the user has configured the extension to receive emails for missed calls, the auto attendant will also send an email about the missed call.

Blacklisted Callers and Anonymous Calls

Once the auto attendant intercepts a call from a blacklisted contact or from a caller who does not have a caller-ID, the caller is required to leave a name. The auto attendant then calls the extension and informs the user of the call. The user can then accept or reject the call. If the call is rejected, it is sent to the mailbox or the busy-extension rules apply. (The caller will hear music while waiting.)

Multiple Messages—Time-Based Configuration

A single auto attendant can be configured to play up to five different messages at different times of day. This is done through the use of service flags (see Chapter 8, "Service Flags"), which must be configured to correspond with the message that is linked to it.

Setting up an Auto Attendant

This section provides instructions for creating and configuring an auto attendant account.

1. From the **Accounts** tab, click **Create** and select **Auto Attendant** from the drop-down.

Create New Accounts:
Accounts are numbers that you can call on the PBX. Please select the account type that you would like to create.
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up several accounts for you. If you use a slash between the names, you will set up one account with different alias names. For example, "123/theo 124/fred" will set up two accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
Auto Attendant
Account Names (e.g. "123/f.feuerstein"):
750

2. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

   ```
   505/9781234567
   ```

   Note: If you use a space instead of a slash (`505 9781234567`), you will create two separate accounts that will be unrelated to each other.

   Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts under accounts page at the domain level (see page 101).

   To create multiple accounts at the same time, use a space between the numbers:

   ```
   505 506 507
   ```

3. Click **Create**.
4. Once the page reloads, click **List**, open the account, and configure it as described in the following sections.

Auto Attendant Behavior

The identity and behavior of the auto attendant (Figure 9-3) are discussed in this section. Identity settings allow you to determine how the auto attendant can be reached by outside callers (e.g., extension number, DID number, or a combination of both). Behavior settings allow you to specify a wide range of settings, e.g., dial-by-name settings, recording settings, and monitoring settings.

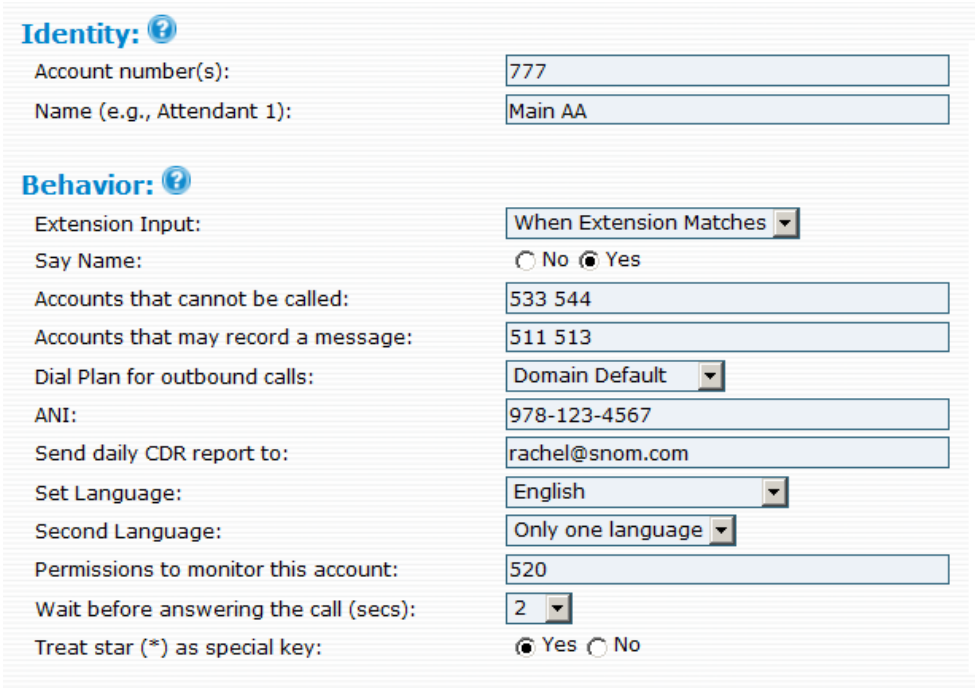
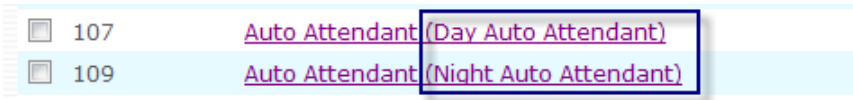


Figure 9-3. Auto Attendant Behavior

Identity

- **Account Number(s)**: This field takes extension number(s) and/or DID number(s). The number of DIDs that can be entered into this field is unlimited.
- **Name**: This field allows you to create an alias so that you can quickly identify the auto attendant among other auto attendants. For example, you might use the names `Day Auto Attendant` and `Night Auto Attendant` to distinguish them from one another.



Behavior

- **Extension Input**: This setting allows you to determine *when* the auto attendant will begin the search for an extension that matches the user's input. The available options are detailed below:
  - When Extension Matches: The auto attendant will wait until the caller's digit sequence matches an existing account. Once the auto attendant finds a match, it will call that extension. This mechanism is useful when accounts of varying name length are used; however, it might be annoying to callers who enter a nonexisting number since the auto attendant will never begin the search.
  - After 1/2/3/4/5 Digit Input: The auto attendant will wait until the correct number of digits has been entered before it will begin looking for an account that matches. If the account does not exist, the system will play an announcement indicating that the extension does not exist.
  - User Must Hit Pound: The auto attendant will wait until the user hits the # sign before searching for an extension. This mode is useful in variable-length scenarios.
- **Say Name**: When this setting is enabled, the system announces the name that was recorded for the account being called. If the user did not record a name, the system will play back the extension number.
- **Accounts that may record a message**: Enter the extensions that are allowed to record auto attendant messages.

  Warning: Leaving this field blank can be risky, as all users will be permitted to record messages, and there is nothing preventing the creation of bogus recordings.
- **Dial Plan for outbound calls**: Choose the dial plan that you would like the system to use when routing calls to an outside provider. (For more information about dial plans, see Chapter 5, "Dial Plans.")
  - Domain default: (This is the dial plan that is on the settings page of the domain.)
  - Outgoing: (You could make it dial plan restrictive.)

- **ANI**: Automatic Number Identification (ANI) is a mechanism that allows phone companies to determine which account should be charged for a call. The ANI is automatically sent to wherever the call is made, and although ANI seems similar to caller-ID, the two are quite different. Caller-ID often reflects the main number of a business, rather than the actual number that made the call. In addition, the ANI shows the class of service of the phone number, while caller-ID shows only the name and number.
- **Send daily CDR report to**: The call data record (CDR) lists all calls that come into the auto attendant. The report is sent nightly at midnight to the email address listed in this field (e.g., voicemail@snom.com). Only one email address is allowed in this field.
- **Set Language**: The auto attendant supports multiple-language environments. You may explicitly specify the language that should be used as the primary language. This setting may differ from the default language in the domain. If you do not select a language, calls that come in from another auto attendant will use its chosen language if that auto attendant's language has been set.
- **Second Language**: If you are operating the system in a dual-language environment (for example, Germany and France), you may want to offer callers a second language. To set this up, use direct destinations, as shown in Figure 9-4. The destination that you send the caller to should have the announced language. If you do not enter a destination, the system will switch the language but continue waiting for input. When a hash sign is placed after a direct destination, the system will wait a few seconds to prevent a conflict with extensions beginning with the same number (in this case, a "1," as shown in the example below).

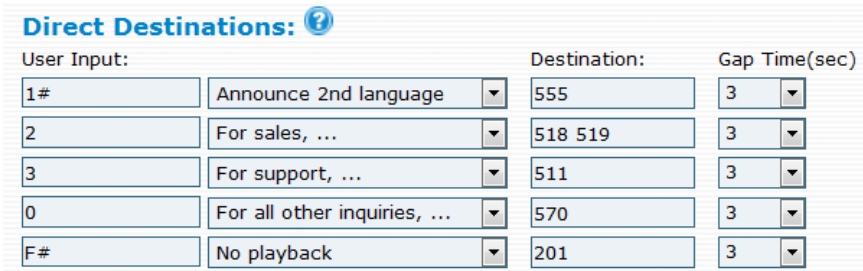
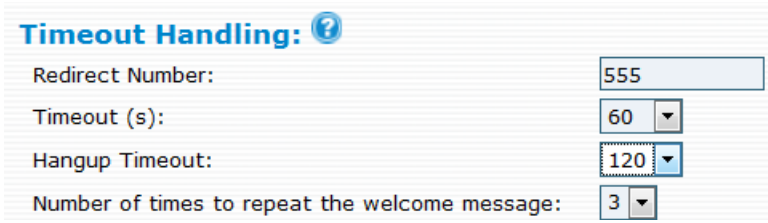


Figure 9-4. Auto Attendant's Second Language Feature

Note: Although the system's language default is limited to two languages, additional languages can be offered by creating multiple auto attendants in different languages. For example, you could set up the first auto attendant to offer a menu of language choices (e.g., "for English, press 1," "for French, press 2," or "for German, press 3"). The first auto attendant would be the English auto attendant, the second would be French, and the third would be German. In a scenario such as this, each auto attendant would be set to its respective language. See "Audio Prompts" in Chapter 18 for more information on audio prompts and languages that can be downloaded.

- **Permissions to monitor this account**: By default, the snom ONE telephone system allows any phone within the domain to monitor an auto attendant account. The account is monitored through the busy lamp field (BLF). To permit only certain extensions to monitor the account, enter those extensions here.
- **Wait before answering the call**: This setting determines the number of seconds that will lapse between the time the system picks up the call and the time the welcome message begins playing. Use this setting if the initial part of the greeting is cut off.
- **Treat star (*) as special key**: This setting allows you to configure the system so that the star (*) key will receive no special treatment when entered by the user, e.g., it cannot be used to redirect the user to the operator. If this feature is deactivated, the star will be treated like any other key (0-9) when the auto attendant is playing a message.

Timeout Handling



The timeout functionality allows you to provide callers with a way to exit the auto attendant when calling from phones with no dual-tone multi-frequency (DTMF) signaling (i.e., Touch-Tone). Without DTMF signaling, callers aren't able to press the auto

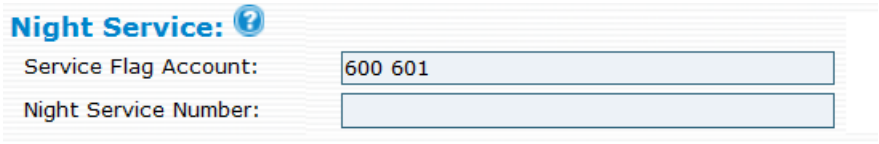
attendant options and would otherwise be stuck. The timeout functionality lets you specify how long the auto attendant should wait before it redirects the call or hangs up.

- **Redirect Number**: This setting allows to you to tell the auto attendant where to direct a call when a caller does not enter the required information within the set timeout period. Enter an extension number into this field.
- **Timeout(s)**: The auto attendant will redirect a caller to the redirect number after a specified number of seconds.
- **Hangup Timeout**: The auto attendant will terminate a call after a specified number of seconds if the user does not enter anything. This feature call help clear a call when the PSTN gateway is not able to detect that the caller has already hung up.
- **Number of times to repeat the welcome message**: This setting determines the number of times the welcome message is played.

Night Service

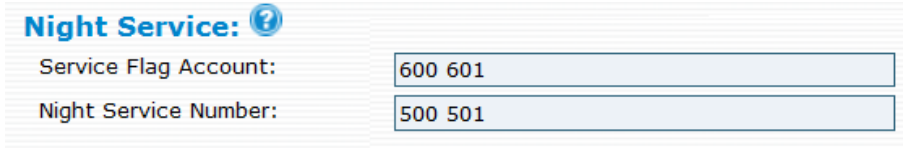
Night service is used to redirect calls to other extensions or phone numbers during certain times of the day/night or other events that are outside normal business hours. Before night service can be used, a Service Flag account must be created for each night service number (see Chapter 8, "Service Flags").

- **Service Flag Account**: Once you have created the service flag account(s), enter the number of the account(s) as shown below.



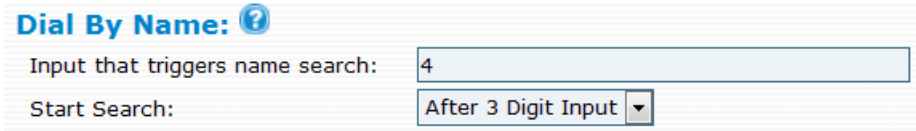
- **Night Service Number**: Once a service flag is in place, the auto attendant can redirect calls directly to the indicated night service number(s). Internal extensions or external number phone numbers may be used in this field.

  Note: You may specify more than one night service flag (separated by a space). The first service flag account will correspond to the first night service number, and the second service flag account will correspond to the second night service number, etc.



Dial-by-Name

The Dial-by-Name feature allows callers to enter numbers from their telephone keypad. The system will search for corresponding names:



- **Input that triggers name search**: Specify the number of digits that a user may enter.
- **Start search**: This setting determines the number of digits that will be required before the system begins searching for corresponding names. When there are several matches, the system will list the available matches in a menu. The caller can always cancel the search by pressing the star (*) key.

Direct Destinations

The Direct Destinations feature is somewhat like a built-in version of the IVR system. To direct inbound calls to specified extensions, you can use the pre-configured destination fields and link them to pre-recorded announcements and user input options. Using the sample shown below, the auto attendant's welcome message will be as follows: "For Sales, press 1. For Support, press 2. For Accounting, press 3. For all other inquiries, press 0." (The user input options are linked to extensions 555, 518, 511, and 570.)

When configuring straightforward, uncomplicated auto attendants, direct destinations are a great solution. However, when configuring auto attendants that require advanced IVR development and functionality, the IVR node is recommended (see Chapter 14).

Once the direct destination links have been established, the system will call the destination number whenever a caller enters the number that is associated with it. In the sample shown above, when the caller presses 1, the call will be connected to extension 555.

By placing a pound sign after the direct destination (e.g., "1#"), the system will wait 3 seconds before dialing the direct destination. This is useful if you have extension numbers in the 100 range (101, 102, etc.). The 3-second delay ensures that the caller's complete input (e.g., 101) will be processed rather than just the first digit.

- **Input number**: This number can be one or multiple digits; however, the system dials direct destinations immediately after a user has provided keypad input, so overlapping between a direct destination and an extension number can be a problem. For example, extensions starting with "1" would conflict with a direct destination of "1" because the system would be unable to dial the extension number. The best way to avoid this situation is to choose extension numbers that do not overlap with either direct destinations or mailbox and outbound call prefixes. The extension range 4xx through 7xx meets these criteria.

  If circumstances render it difficult to change the extension assignments (e.g., business cards with extension numbers already in circulation), a timeout mechanism can be used. By placing a pound sign after the direct destination (e.g., "1#"), the system will wait for 3 seconds before dialing the destination.

  To redirect fax messages to a specific destination, you can use the direct destination "F". The CNG tone that announces a fax tone is recognized by the system and is translated into the "F" key.

- **Destination**: This number can be either an internal number (e.g., an extension or conference room) or an external number.

  When more than ten direct dial options are needed, auto attendants can be nested within one another, as shown in the next section.

- **Gap time**: This setting determines the number of seconds that will lapse between the different audio options: e.g., "For sales, press 1" (3 seconds), "For accounting, press 2" (3 seconds), etc.

Nesting Auto Attendants

Nesting auto attendants within other auto attendant allows for a sophisticated hierarchy of information. Figure 9-5 depicts three auto attendants nested within the main auto attendant. This model could be developed even further to include nine additional auto attendants, one for each of the boxes shown to the right (i.e., an auto attendant could be created for product A that would include prompts that are specific to that product).

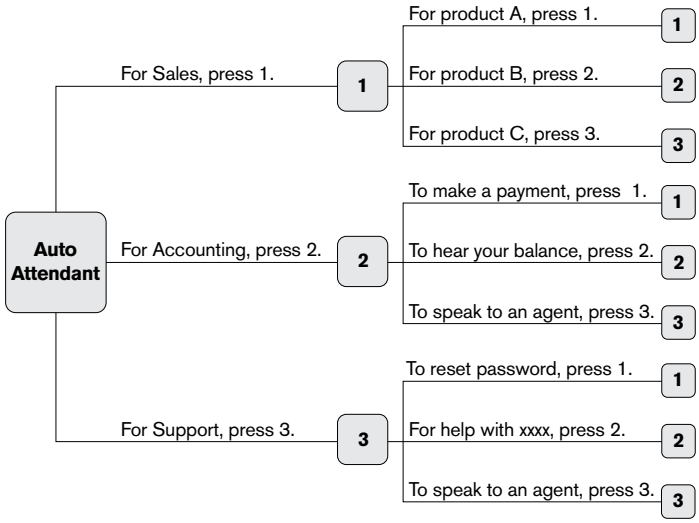


Figure 9-5. Nested Auto Attendants

To create a nested auto attendant, individual auto attendant accounts must be set up (see "Setting up an Auto Attendant Account" on page 198). Using the model shown

in Figure 9-5, four auto attendant accounts are needed. Extension 554 can be the main auto attendant, and extensions 555, 556, and 557 can be nested within it (Figure 9-6).

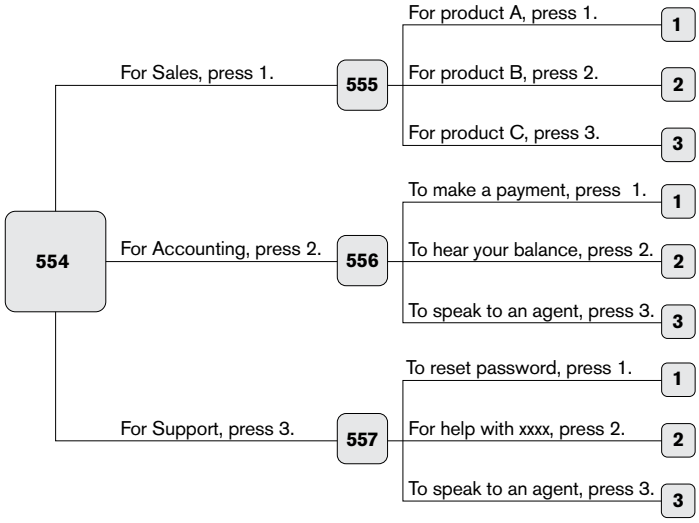


Figure 9-6. Nested Auto Attendants and Direct Destinations

To "nest" the three auto attendants within the main auto attendant, they must be listed as direct destinations of the main auto attendant.

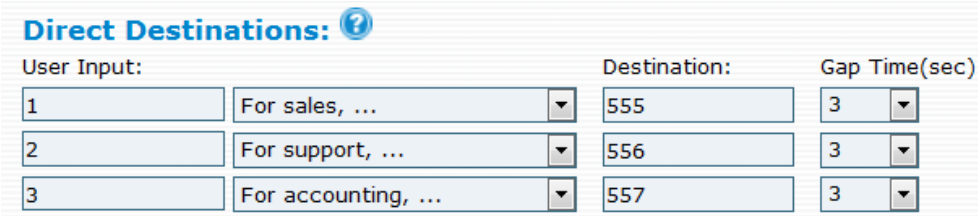


Figure 9-7. Direct Destination Settings from Web Interface

Welcome Greetings

Overview

From the auto attendant's IVR settings (Figure 8-8), you can configure the account so that you can control which announcement plays when callers reach the auto attendant. A single auto attendant to play up to five different messages at different times of day. For each greeting, a service flag (see Chapter 8, "Service Flag") and a corresponding greeting is needed. You can either upload a WAV file or record a greeting using the Record Greeting (*98) star code.

To set up the auto attendant's messaging system, follow these steps:

1. Open the auto attendant account and click **IVR**:

2. Enter your greeting into the system either by recording the message using the star code (*98) or by uploading it as a WAV file. See the next section, "Recording the Greeting."

Recording the Greeting

Before an extension can record a greeting for an auto attendant account, the extension must have permission to do so. The permission setting can be found in the auto attendant account and is called **Accounts that may record a message**.

Once an extension has permission, greetings can be recorded using the Record Greetings star code (*98). They can also be uploaded as a WAV file by anyone with permission to access the account.

To record greetings using *98:

1. From the telephone keypad, enter *98.
2. Enter the auto attendant account number.
3. Enter the greeting number following by the star key (e.g., 1*).
4. Press the confirm button.
5. The greeting will automatically be assigned to that auto attendant.

6. Repeat these steps for each greeting, recording a new greeting each time (e.g., *2, *3, etc.).

   The greetings will appear in the **Current File** field as shown below:

Note: When a single greeting will be used for all calls, you do not need to specify a greeting number when using the *98 star code. This greeting is considered the default greeting and will not appear in the **Current File** field.

To record greetings by uploading WAV files:

1. Using a recording device, record the greeting (use an 8 kHz mono, 16 bit file).
2. Go to the auto attendant's **IVR** tab and click **Browse**.
3. Select the recorded file.
4. Click **Save**. The file will be placed into the `snom/snomONE/recordings` directory.

Filing System and Naming Conventions

All greetings are automatically placed into the `recordings` directory whether they have been recorded using *98 or uploaded into the system through the web interface. Unlike uploaded greetings, which can be named according to a user's preference, greetings that have been created with *98 are named according to the system's syntax rules. Its naming system is based on the greeting number that was recorded and the account type (personal, auto attendant, agent group, etc.) from which it was recorded. However, the actual account number is never reflected in the file name of the greeting. For example, if a user creates a personal greeting using *98*1, then the file could be named `personal10-1.wav`, `personal23-1.wav`, `personal24-1.wav`, etc. (the numbers 10, 23, and 24 are internal user IDs and could actually be any number).

Table 9-2. Automatic Naming Conventions for *98 Greetings

Account Type	Input	Internal Naming System	File Name
Personal	*98*1	personal<internal user ID>-1.wav	`personal10-1.wav`

Account Type	Input	Internal Naming System	File Name
Personal	*98*2	personal<internal user ID>-2.wav	`personal10-2.wav`
Auto attendant	*9870*1	att1_<internal user ID>.wav	`att1_11.wav`
Auto attendant	*9870*2	att2_<internal user ID>.wav	`att2_11.wav`
Agent group	*9873*1	att2_<internal user ID>.wav	`acd1_14.wav`
Agent group	*9873*4	att2_<internal user ID>.wav	`acd4_14.wav`

Note 1: Internal user IDs are generated by the system.

Note 2: Numbers in blue indicate account numbers.

Greetings can be viewed from either the Windows environment (Figure 9-8) or the command prompt (Figure 9-9).

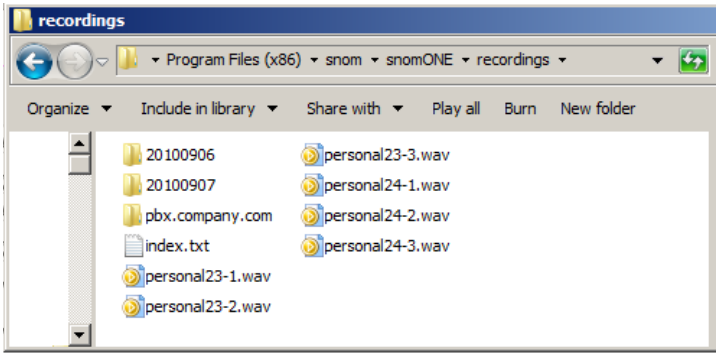


Figure 9-8. Viewing Greetings from the Windows Environment

To view greetings from a command prompt, open a command prompt and navigate to the following path: `C:\snomONE\snom\recordings`. When navigating, you can use the following steps:

1. `cd ..` (this will step you back a directory; you may need to repeat this command if you are not at the C prompt yet)
2. `cd Program Files`

3. `cd snom`
4. `cd snomONE`
5. `cd recordings`
6. `dir` (this will show the list of WAV files)

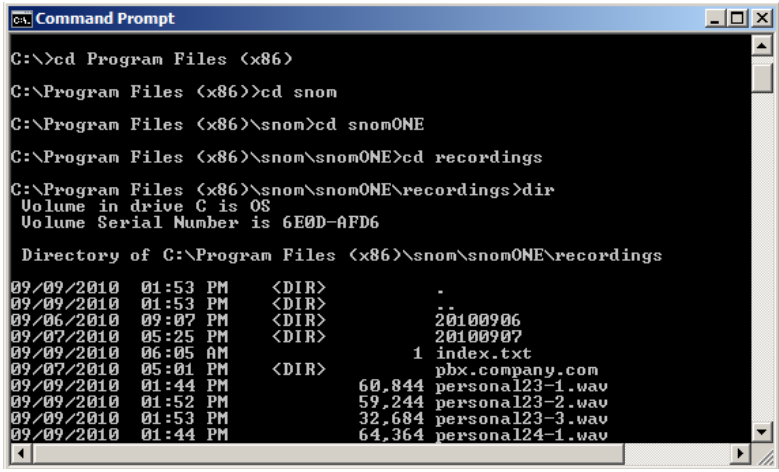
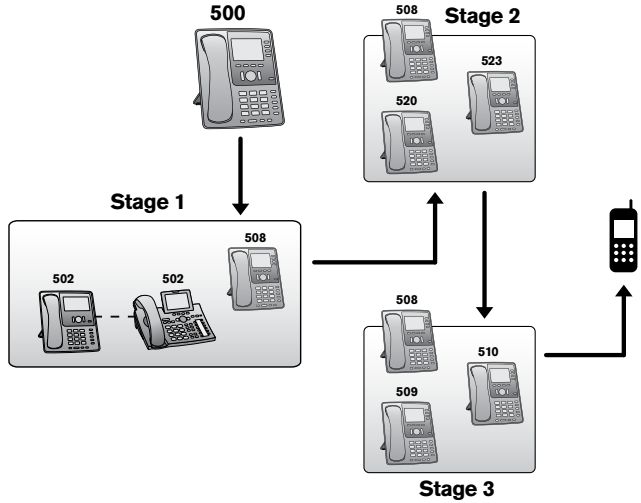

Command Prompt
C:\>cd Program Files (x86)
C:\Program Files (x86)>cd snom
C:\Program Files (x86)\snom>cd snomONE
C:\Program Files (x86)\snom\snomONE>cd recordings
C:\Program Files (x86)\snom\snomONE\recordings>dir
Volume in drive C is OS
Volume Serial Number is 6E0D-AFD6
Directory of C:\Program Files (x86)\snom\snomONE\recordings
09/09/2010 01:53 PM <DIR> .
09/09/2010 01:53 PM <DIR> ..
09/06/2010 09:07 PM <DIR> 20100906
09/07/2010 05:25 PM <DIR> 20100907
09/09/2010 06:05 AM 1 index.txt
09/07/2010 05:01 PM <DIR> pbx.company.com
09/09/2010 01:44 PM 60,844 personal23-1.wav
09/09/2010 01:52 PM 59,244 personal23-2.wav
09/09/2010 01:53 PM 32,684 personal23-3.wav
09/09/2010 01:44 PM 64,364 personal24-1.wav

Figure 9-9. Viewing Greetings from the Command Prompt

Chapter 10

HUNT GROUPS

A hunt group is a set of extension numbers that are embedded inside a single virtual extension. Incoming calls are rotated through the pool of extensions until someone answers and the caller is connected. (Cell phones can also be configured to be included in calls made to a hunt group.)



The extension numbers that are part of a hunt group can be arranged into groups known as *stages*. Each stage is configured to ring for a specified period before the system begins ringing the next stage. A last-resort or final stage number (often an auto attendant or a cell phone) can also be used when none of the extensions pick up the call. A common use case for the hunt group is to use the hunt group as the main number

for incoming calls, then put the receptionist, secretaries, and assistants on the different stages.

Table 9-1 lists the hunt group features.

Table 10-1. Hunt Group Features

Feature	Functionality	Benefit
Custom ringing	Each hunt group can be configured with different ring tones.	Employees can determine which hunt group is calling.
BLF indicator	The system can be configured so that the busy lamp field indicator lights up when the hunt group is in use.	Hunt group activity is visible through the BLF indicator.
Group name caller-ID	Hunt groups can have a unique name and can be configured to display the name of the group, the caller's caller-ID, or both when a caller enters a hunt group.	Helps management decide who belongs in each named group. Employees know the nature of the call before answering it.
Three-stage extension ringing	Hunt groups can be configured to ring 1–3 different groups of extensions. The system will ring each group in succession until the call is answered.	Managers can direct calls to selected groups of extensions in a specified order.
Final stage to cell phone	After calling the extensions listed in stages 1 through 3, the system calls the "final stage" number, which can be an auto attendant, an extension, or an external number.	Callers are sent to a manager as a final means of assistance. This feature can also be used to gauge whether the group of extensions is too small or whether the employees are working properly.
Ring stage duration	Hunt group stages can be configured to ring for different durations before the system rings the next group of extensions.	Call flow control can be established. Intervals that keep customers waiting a minimum amount of time can be used.

Feature	Functionality	Benefit
Recordable calls	Calls made to hunt groups can be recorded and saved on the system.	Recorded calls can be reviewed by management to fine-tune employee performance. Disputes can be easily resolved by emailing the recorded conversation.

How the Hunt Group Works

Once a caller has reached a hunt group, the system begins searching for an extension that will answer the call. Hunt groups can be configured with one to three stages of extensions, and each stage can consist of any number of extensions. When looking for an extension, the system begins with stage 1. Once the ring stage duration has been met (page 220), the system stops ringing that group of extensions and begins ringing the next stage. This scenario continues until all extensions in all stages have been called.

As a last-case scenario, the system rings the "final stage" number, which in this case is a cell phone (Figure 10-1). The final stage number is often an auto attendant or a manager's cell phone number.

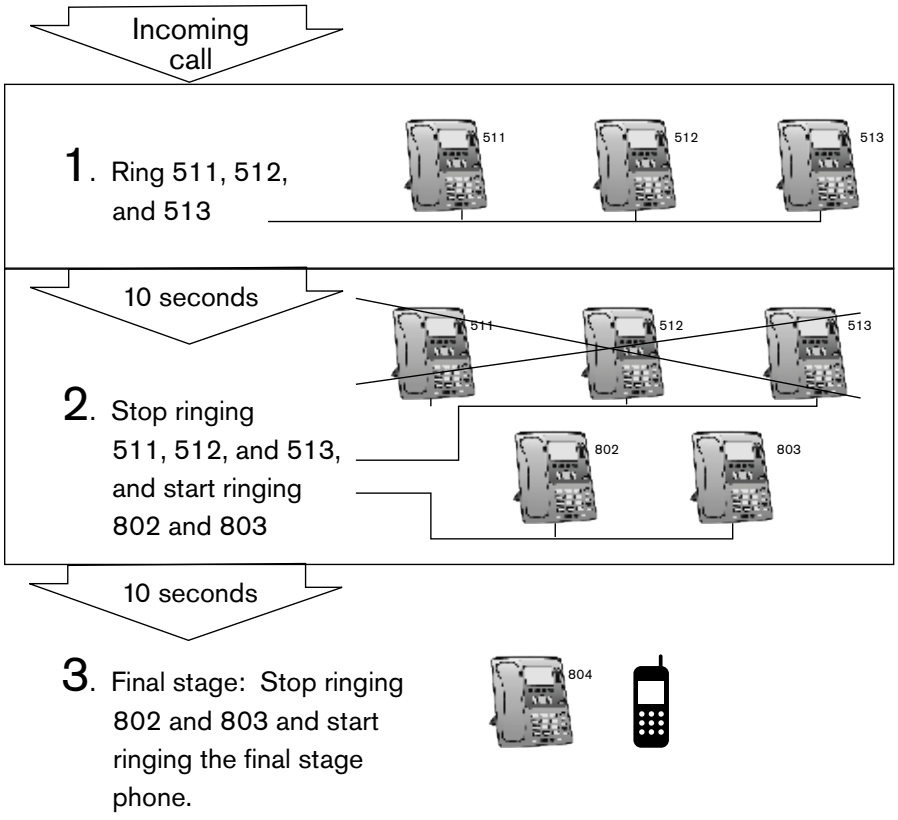


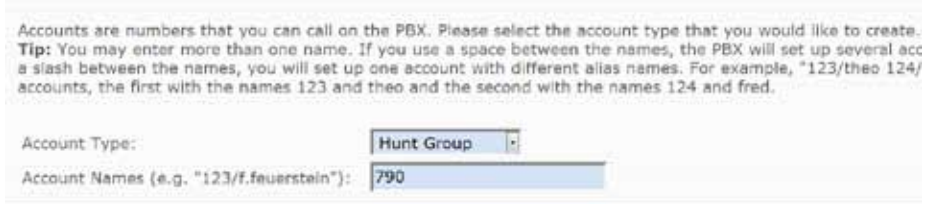
Figure 10-1. Hunt Group Call Flow

Note: If an extension belongs to more than one stage, the extension will continue to ring through each stage.

Setting up a Hunt Group

This section provides instructions for creating and configuring a hunt group account on the snom ONE telephone system.

1. From the **Accounts** tab, click **Create** and select **Hunt Group** from the drop-down:


Accounts are numbers that you can call on the PBX. Please select the account type that you would like to create.
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up several acc
a slash between the names, you will set up one account with different alias names. For example, "123/theo 124/
accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
Hunt Group
Account Names (e.g. "123/f.feuerstein"):
790

2. In the **Account Name** field, enter an extension number and/or alias, i.e., a **DID** number. When entering an alias in addition to an extension number, use the following syntax:

   ```
   505/9781234567
   ```

   Note: If you use a space instead of a slash (`505 9781234567`), you will create two separate accounts that will be unrelated to each other.

   Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this happens, you can **hide aliased accounts under accounts page** at the domain level (**Domain** > **Settings**).

   To create multiple accounts at the same time, use a space between the numbers:

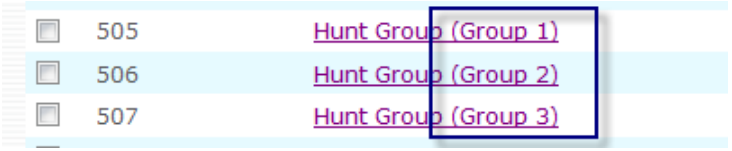
   ```
   505 506 507
   ```

3. Click **Create**.
4. Once the account has been created, click **List** to open the account and configure it as detailed in the following sections.

Identity

The identity settings allow you to identify the hunt group to hunt group members who are receiving the calls and to managers who are monitoring the account.

- **Account Number:** This field takes extension number(s) and/or DID number(s). The number of DIDs that can be entered into this field is unlimited. This information can be changed at any time.
- **Name**: This field allows you to name the hunt group. The name allows hunt group members to differentiate between calls coming into the hunt group and calls not associated with it. Choose a short name if you plan to use the **Group name (calling party)** option in the `From` header to ensure that it will fit into the display of the phone. This field also distinguishes one hunt group from another hunt group on the **Accounts** page.



Ring Stages

The hunt group supports three stages and a final stage. Each stage can be configured to ring for a different number of seconds, and the final stage can be either an internal or external phone number.

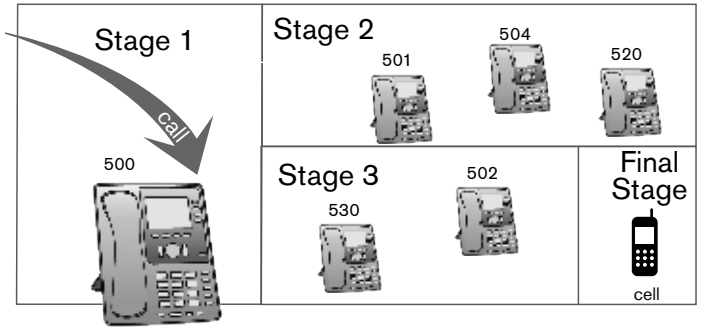
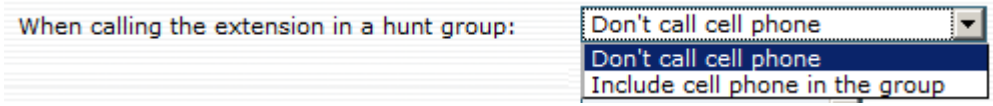


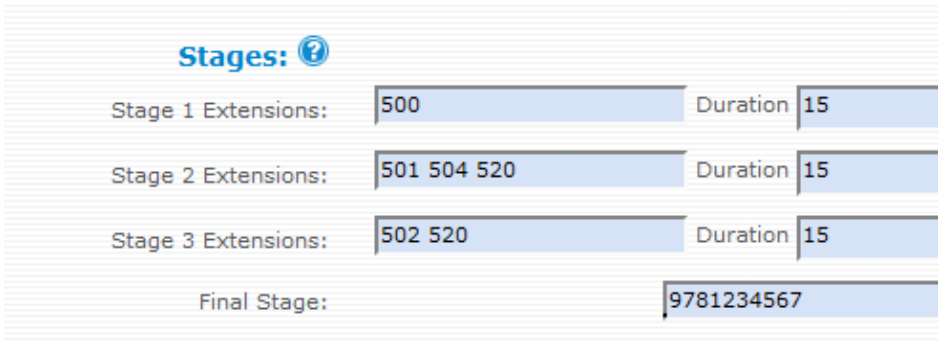
Figure 10-2. Hunt Group Search Activity

If an extension has configured a cell phone and has enabled the **When calling the extension in a hunt group** setting (page 468), the hunt group will also ring that person's cell phone.



For each stage:

1. List the extensions that should be part of that stage. When entering multiple extensions, use a space as a separator (only one number is permitted for the final stage).
2. For duration, specify the length of time that the system should ring each stage before ringing the next. The duration of the stages must be specified in seconds.
3. For unwanted stages, leave the fields empty.

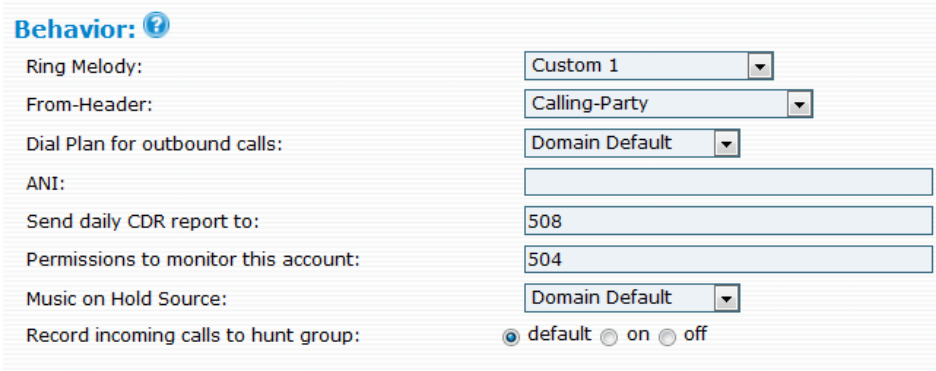


If all extensions of a stage are unavailable, the system will immediately move to the next stage.

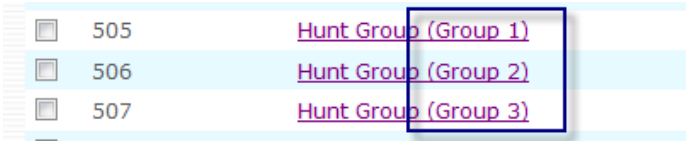
Note: The number of extensions permitted for the first three stages is limited by hardware only. The system must send INVITEs to all extensions in each stage, which requires more CPU.

Behavior

Behavior settings allow you to control numerous account behaviors. You can choose a ring melody, a display header, and music on hold source. You can also enter a safety net phone number that will be used if no one picks up a call. Other settings are here as well.



- **Ring Melody**: This setting allows you to set the ring melody so that hunt group members will be able to distinguish regular calls from hunt group calls.
  - Custom 1 through 4: Custom ringtones allow users in a hunt group to distinguish hunt group calls from other calls. Before customized ringtones can be used, you will need to provide your own ringtones, modify the `ringtones.xml` file, then place it into the `html` directory. When the phones receives the `alert-info` header from the system, it will respond with a different ring tone based on the ringtone that was selected from the web interface. For instructions on configuring custom ringtones, see "Customized Ringtones" in Chapter 18.
  - External Call: The ring tone will be long.
  - Internal Call: This ring tone will be short.
- **From Header:** This setting allows you to set the display name that hunt group members will see when someone is calling. Four options are available:
  - Calling party: This mode displays the calling party.
  - Group name: This mode displays the name of the hunt group that was called:



  - Group name (calling party): This mode displays both the group name and the calling party.
  - Calling party (CMC): The calling party's client matter code will appear in the display, if one is available. The CMC identifies the customer and is used to expedite billing in offices that bill their clients for phone calls.

- **Dial plan for outbound calls**: Select the dial plan that will be used for this account.
- **ANI**: The hunt group uses an ANI (automatic number identification) when sending a caller to an external number. This setting is necessary when the user input handling destinations take callers to external numbers rather than extension numbers within the domain.
- **Send daily CDR report to**: The call data record (CDR) lists all calls that come into the hunt group. The report is sent at midnight each night to the email address listed in this field (e.g., voicemail@snom.com). Only one email address is allowed in this field.
- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this hunt group account.
- **Music on hold source**: From the dropdown list, choose the music that callers will hear while waiting.
- **Record incoming calls to hunt groups**: When this setting is enabled, the system will record all calls that come into the hunt group. The recordings can later be retrieved and reviewed.

Night Service

Night service allows you to redirect calls to other extensions during off-hours, meetings, etc. Before you can use night service, you need to create a Service Flag account (see Chapter 8).

- **Service Flag Account**: Once you have created the account, enter the number of the account as shown below.

- **Night Service Number**: With a service flag in place, the hunt group can redirect the calls directly to the night service number(s) shown in this field. Internal extensions and external numbers are acceptable.

  Note: You may specify more than one night service flag (separated by a space). The first service flag account will correspond to the first night service number, and the second service flag account will correspond to the second night service number, etc.

  Note: You can also use a special character pattern (#L) to activate the service flag when all agents are logged out, even if the logout period is within normal working hours. All calls will automatically be redirected to the specified night service number(s).

Chapter 11

AGENT GROUPS

An agent group, also known as automatic call distribution, is a system that routes incoming calls to a specific group of agents. Before connecting to an agent, callers are placed inside a queue, allowing agents to deal with incoming calls without losing other callers to busy signals or unanswered phones. While waiting, callers hear music and pre-recorded announcements.

Agent groups are often found in offices that handle high-volume customer calls from callers who do not need to speak with a specific person but who require assistance from any of multiple persons, like sales representatives and airline reservations attendants.

Agents must log into the queue to begin receiving calls. When agents have finished for the day or would like to stop receiving calls from the queue, they must log out of the queue.

The following features are available with the agent group:

Table 11-1. Agent Group Features

Feature	Functionality
Display name	Each agent group can have a distinct name that will appear on the telephone display when calls come in. This allows calls to be properly answered and tracked.
Ring melody	Each agent group can have a unique ring melody so that agents can distinguish which agent group is ringing.
Jump in and out	Agents may jump in and out of any group to which they are assigned. This allows managers to dynamically adjust to a changing workload.

Feature	Functionality
Minimum number of agents	Managers can establish a minimum number of agents that must remain in a group. This ensures that an agent will always be available and that calls will be answered.
Number of agents per stage	You can create a comfortable balance of waiting and connecting within agent groups by setting the number of agents who can receive calls at the same time.
Record agent group calls	Calls that come into agent groups can be recorded, and recordings can be reviewed and emailed later on.
Call distribution methods	Calls can be distributed to agents randomly, according to most idle, or according to skill level. Experienced agents can be used to answer calls first. Agents with fewer skills can be held in reserve.
Recovery time	Recovery time gives each agent a period of time to prepare for the next incoming call.
Auto add callers to address book	Callers can be automatically added to the address book, making it easier to return phone calls.
Caller priority	For repeated callers, the system rings the agent who provided assistance on the last call. If the agent is not available, the caller will be sent to the next available agent. Caller priority helps callers maintain continuity.
Music on hold	To help set the mood for a particular agent group, distinct music can be provided for each agent group. Callers can hear music that relates to their call (e.g., classical music for callers looking to buy classical music, jazz for those looking to buy jazz, etc.).
Multiple announcements	Messages can be delivered to callers while waiting inside an agent group, allowing you to present additional services or products.
Gaps between announcements	The amount of time between agent group announcements can be controlled. During this gap time, the caller will hear music. This allows you to set up attention-getting sequences.
Agent group queue manager	An agent group manager can be designated for each agent group. Queue managers can monitor agent group queues.
Send daily reports	Nightly activity reports are delivered to selected email addresses. This allows management to review the previous day's information.

How the Agent Group Works

A caller reaches an agent group in one of two ways: either by calling the agent group directly or by calling a company's auto attendant. When agent groups branch off the auto attendant, callers must press the number that corresponds with their choice. In Figure 11-1, the caller has reached an auto attendant offering three different choices: Sales, Accounting, and Support. The caller hears these options in the form of pre-recorded messages. Each option will connect the caller to an agent group, and the caller will be placed inside a queue until an agent becomes available.

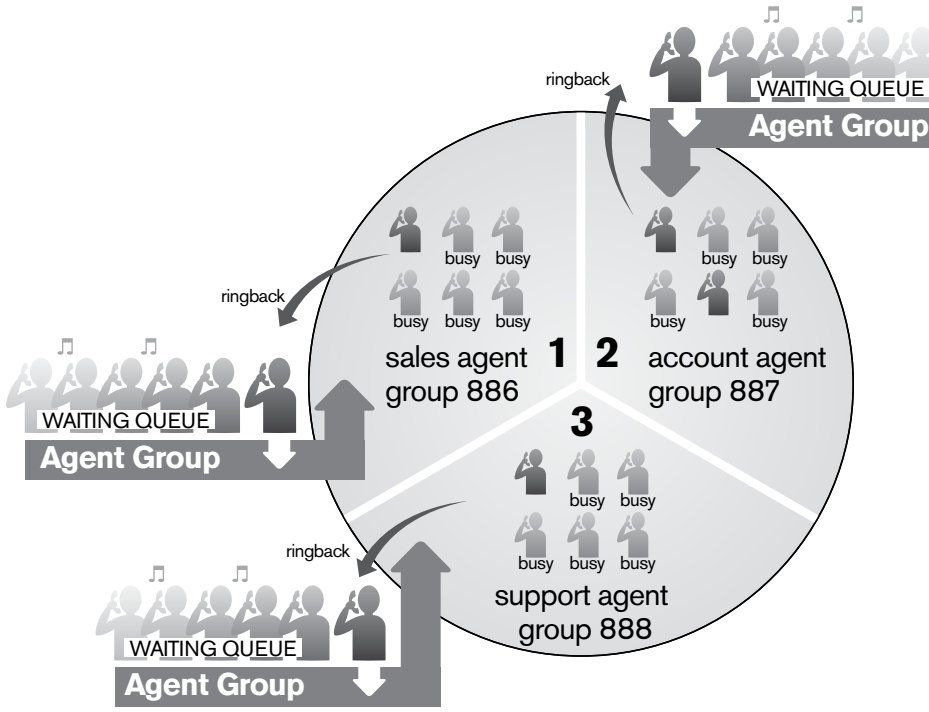


Figure 11-1. Agent Group Queueing

The Message-Music Cycle

While the caller is waiting, the system delivers a combination of pre-recorded messages and music. The messages can be used to provide additional information about your

company, or they can be used to provide the caller with additional options and/or a way to exit the queue. Each agent group can be configured to play up to nine recorded messages.

Between the messages are "gaps" of music which can be configured to span 5 to 180 seconds. This message-music cycle continues for as long as the caller is in the queue. Message 0 is considered the entry point message (which will never be replayed), and message 1 is the first message. Figure 11-2 shows an agent group using six different messages for its message-music cycle. Once message 6 has been played, the system returns to message 1 and repeats the cycle.

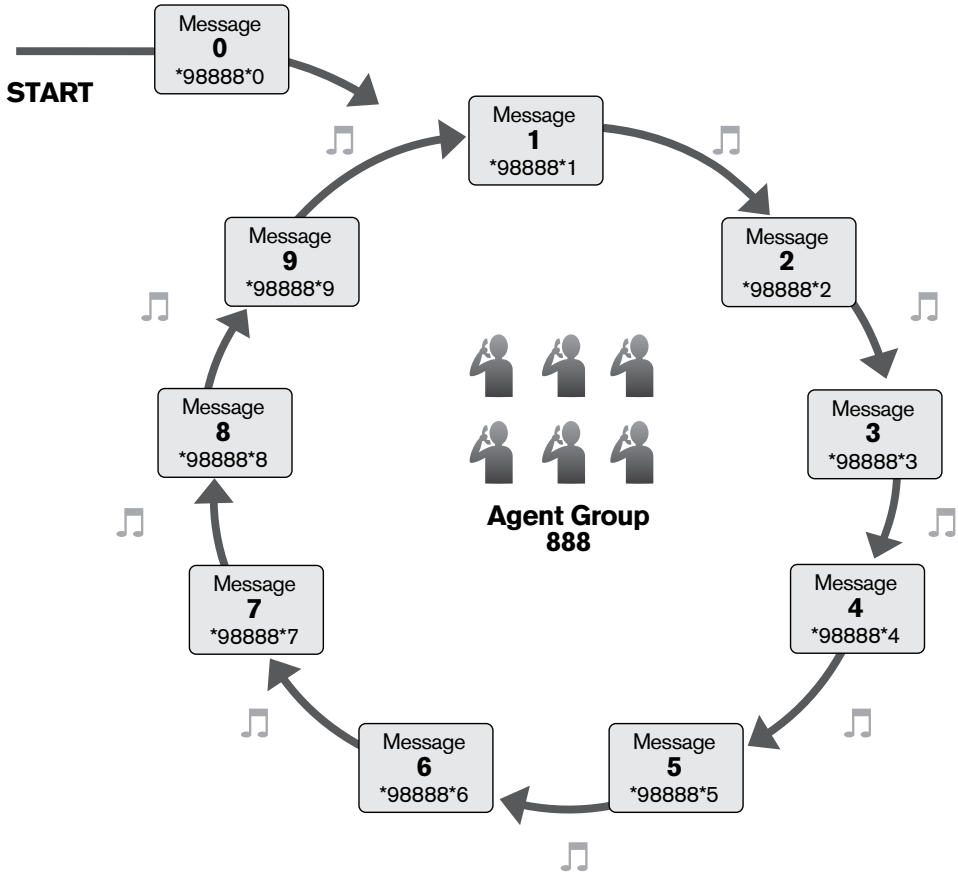


Figure 11-2. Messages Alternating with Music

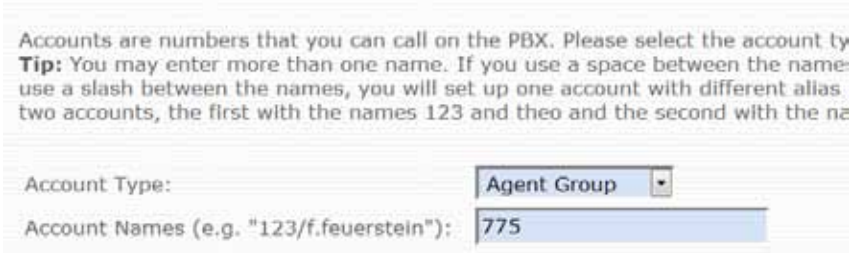
As previously mentioned, this sequencing of messages and music will continue until an agent becomes available. Once an agent is available, the system automatically takes the next call out of the queue, rings the agents, and puts the call into ringback state. Within any one agent group, only one call at a time can be in ringback state, regardless of the number of agents that are available. All other calls remain queued until the ringing call is connected and at least one agent becomes available.

While it might seem logical to conclude that a caller's time in the queue has ended once the call has been placed in ringback state, this is not always the case. If an agent leaves the desk without logging out of the queue, the ringback state will continue until the system finds another agent to answer the call. To prevent nonstop ringing, you can take two precautions: (1) you can configure the agent group to include additional agents at specified intervals in the ringback cycle and (2) you can configure the agent group to play music *during* the ringback state. This will prevent the caller from hearing long periods of ringing in the event there are episodes of extended ringback.

Setting up an Agent Group Account

This section provides instructions for creating and configuring an agent group account.

1. From the **Accounts** tab, click **Create** and select **Agent Group** from the drop-down:


Accounts are numbers that you can call on the PBX. Please select the account ty
Tip: You may enter more than one name. If you use a space between the name
use a slash between the names, you will set up one account with different alias
two accounts, the first with the names 123 and theo and the second with the na
Account Type:
Agent Group
Account Names (e.g. "123/f.feuerstein"):
775

2. In the **Account Name** field, enter an extension number and/or alias, i.e., a **DID** number. When entering an alias in addition to an extension number, use the following syntax:

```
775/9781234567
```

Note: If you use a space instead of a slash (`775 9781234567`), you will create two separate accounts that will be unrelated to each other.

Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts under accounts page at the domain level (**Domain** > **Settings**).

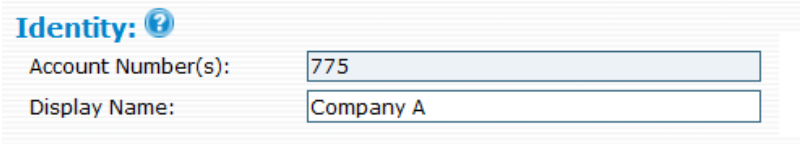
To create multiple accounts at the same time, use a space between the numbers:

```
775 776 777
```

3. Click **Create**.
4. Once the page reloads, click **List**, open the account, and configure it as described in the following sections.

Identity

The identity settings allow you to identify the agent group to both agent group members who are receiving the calls and managers who are monitoring the account.



- **Account Number:** This field takes extension number(s) and/or DID number(s). The number of DIDs that can be entered into this field is unlimited. This information can be changed at any time.
- **Display Name:** This field allows you to name the agent group. The name allows agent group members to differentiate between calls coming into the agent group and calls not associated with it. Choose a short name if you plan to use the **Group name (calling party)** option in the `From` header to ensure that it will fit into the display of the phone. This field also distinguishes one agent group from another agent group on the **Accounts** page.

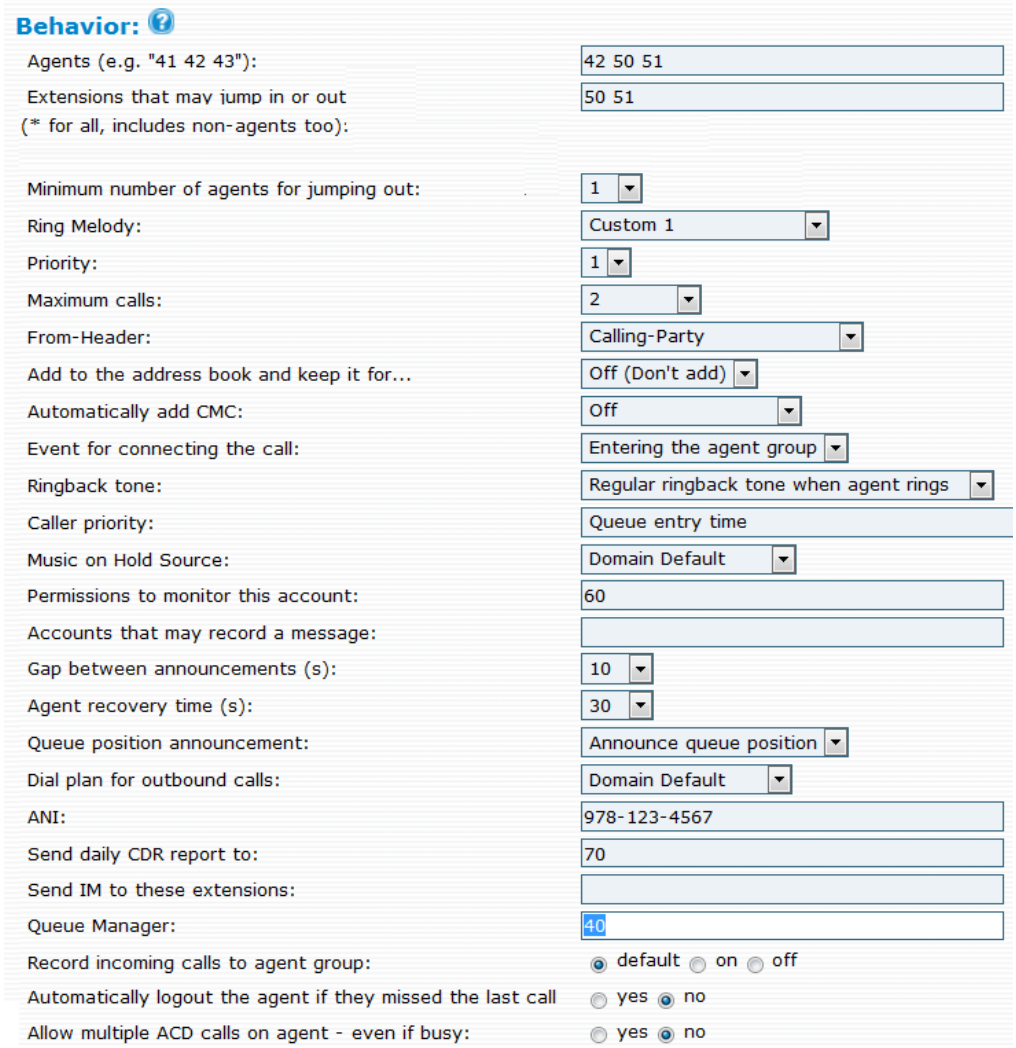
Behavior

Behavior settings allow you to control numerous account behaviors. You can set a ring melody, music on hold, and a display header. You can also specify who will monitor the account, manage the queue, and receive the daily Call Detail Record (CDR). Gaps between announcements, agent recovery time, and the number of agents allowed to jump in and out of the agent group can also be set here.

- **Agents**: Enter the extension numbers of the agents who will comprise the agent group. Extension numbers should be entered in the order in which the system should call them. This field can also be left empty; however, callers waiting in queue will need to be pulled out manually using the Call Pickup feature.
- **Extensions that may jump in or out (* for all)**: This setting controls which agents can dynamically join or leave the agent group. It can also be used to add non-agents to the agent group, which can be useful during especially busy periods when additional people are needed for the queue. If a star is used in this field, extensions that use *64 will automatically be listed in this field, i.e., the list will grow and decrease as people log in and out. It is recommended that actual extensions be entered into this field.
- **Minimum number of agents for jumping out**: This setting specifies the number of agents that must remain in the agent group before agents are permitted to jump out. If this setting is too high, agents will be unable to log out of the agent group. For small agent groups, a value of `1` is recommended.
- **Ring Melody**: It is important to set the ring melody so that the phone knows which one to play and so that agents will be able to distinguish regular calls from agent group calls.
  - Custom 1 through 4: Custom ringtones allow users in an agent group to distinguish agent group calls from other calls. Before customized ringtones can be used, you will need to provide your own ringtones, modify the `ringtones.xml` file, then place it into the `html` directory. When the phone receives the `alert-info` header from the system, it will respond with a different ring tone based on the ringtone that was selected from the web interface. For instructions on configuring custom ringtones, see “Customized Ringtones” in Chapter 18.

  - External Call: The ring tone will be long.
  - Internal Call: This ring tone will be short.

- **From-Header**: This setting allows agents to see who the call is coming from. By default, the name of the calling party is displayed, but the system can be configured to display the name of the queue (see Display Name in this chapter), either by itself or with the calling party. When both are shown, the system puts the caller-ID in brackets after the display name. This mode requires that the phone have enough space to display a long number. When using this mode, choose a short group name so that it requires less space.
  - Calling party: The calling party is shown in the display.
  - Group name: The name of the agent group queue (which is set in the Display Name field) is shown in the display.
  - Group name (calling party): Both the calling party and the agent group queue are shown. (The caller-ID appears in brackets after the agent group name.) When using this mode, choose a short group name to ensure that it will fit in the phone display.
  - Calling party (CMC): The calling party's client matter code will appear in the display, if one is available. The CMC identifies the customer and is used to expedite billing in offices that bill their clients for phone calls.
- **Add to the address book and keep it for . . .** : Automatically adding a caller's phone number into the address book allows the caller, when calling again, to be routed to the same agent.
- **Automatically add CMC**: When this feature is turned on, the caller's **CMC** will appear in every CDR that is written on the disk. The CMC is used for automatic billing.



- **Event for connecting the call**: This setting allows you to tell the system when to pick up the line if the line has not been picked up already (for example, by an auto attendant).
  - Entering the agent group: The call is picked up when it enters the agent group. In most cases, this is suitable behavior.
  - Music playback: If the caller has to wait for an available agent, the caller is put on hold and hears music while waiting. If the call goes directly to

an agent, the queue waits until the agent picks up the call before connecting it.

  - Agent picks up call: The call is not connected until the agent picks up the call, even if music on hold and/or announcements have been set. This option is useful if the waiting time in the queue is typically very short and there's no risk of the carrier disconnecting the call due to no answer.
  - Never connect: The call is never connected. This is useful if you want to provide free services to callers. This setting prevents the carrier from seeing the call. As with the other options, there is a risk that the carrier will not tolerate this behavior and will hang up the call after a certain timeout.

- **Ringback tone**:
  - Regular ringback tone when agent rings: The caller will hear the agent ringing.
  - No ringback tone, continue playing music: Instead of hearing a ringback tone, the caller will hear music. If an agent is no longer at his desk but has not logged out of the agent group, the caller will hear music on hold instead of ringback.
- **Caller priority**: This feature allows callers to be connected to agents who have handled their calls in the past.
  - Queue entry time: All callers will be placed in queue and will remain there until an agent becomes available.
  - Try to pull out callers when their last agent becomes available: Callers will be pulled from the queue if their last agent becomes available.
- **Music on Hold source**: From the dropdown list, choose the music that the caller will hear while waiting for an agent.
- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this agent group account.

- **Accounts that may record a message**: Specify which accounts may record announcements. When this setting is left empty, all extensions will have permission to record announcements.
- **Gap between announcement(s)**: From the dropdown list, select the number of seconds that the system should wait between each announcement.
- **Agent recovery time(s)**: Use this setting to ensure that an agent has adequate time to recover from the previous call before taking another call. In busy call centers, 2 seconds might be an appropriate setting. However, agents who are required to record notes about the call will need a longer value. In these cases, 60 seconds might be more appropriate. The recovery time also allows an agent to log out of the agent group.
- **Queue position announcement**: When **Announce queue position** is selected, an announcement will let callers know their position in queue.
- **Dial plan for outbound calls**: Select the dial plan that will be used for this account. For more information on dial plans, see Chapter 5, "Dial Plans."
- **ANI**: The agent group uses an ANI (automatic number identification) when sending a caller to an external number. This setting is necessary when the user input handling destinations take callers to external numbers rather than extension numbers within the domain.
- **Send daily CDR report to**: The call data record (CDR) lists all calls that came into the agent group on the previous day. The report is sent at midnight each night to the email address listed in this field (e.g., `Fred Feuerstein <ff@domain.com>`). Only one email address is allowed. It you want to send the CDR email immediately, click the **Try** button, rather than waiting until midnight. Keep in mind that this is just a link, and you may have to save your list before clicking the link. For sample CDR reports, see Figure 11-4 and Figure 11-5.
- **Send IM to these extensions**: The agent group queue can be monitored from SIP phones that support the SIMPLE standard for instant messaging and presence. Multiple extensions are permitted in this field (use a comma as a space separator). Phone models with larger screens will be able to display the full message.

- **Queue Manager**: This setting allows you to assign an extension as queue manager. Once an extension has been designated, the agent group's identity must be listed in the extension's **Show following ACD queues** field, as shown below. This configuration is set from the user's extension account.

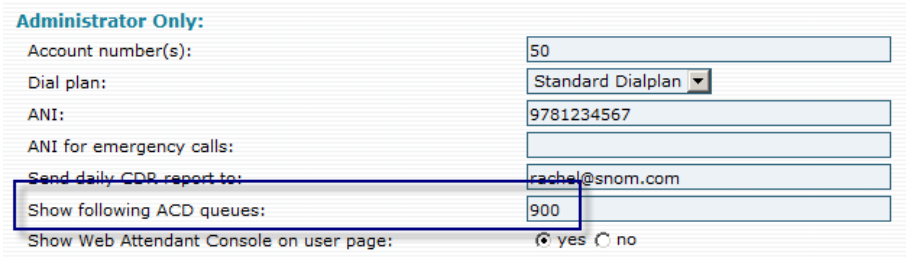


Figure 11-3. Permission to be Queue Manager

Once access to the status queue has been given, the queue manager will be able to view important information about the calls. Information includes whether anyone "escaped" out of the queue to connect to other destinations, the length of time each caller spent in the queue, and the length of time the caller spent talking. Information about the agents is also shown in the report (e.g., agents in the queue and number of calls handled by each agent). The queue manager can access the information from the **Status** tab (user account). The information is refreshed every 10 seconds.

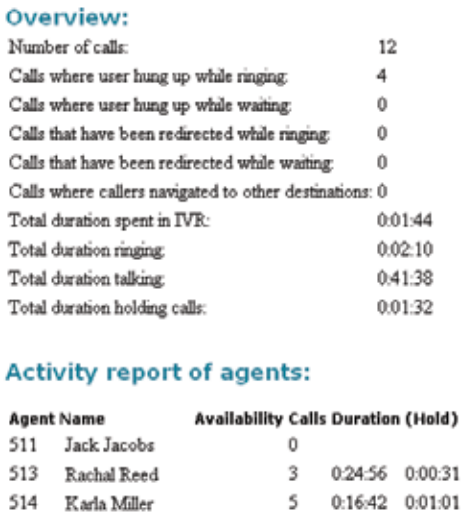

Overview:
Number of calls: 12
Calls where user hung up while ringing: 4
Calls where user hung up while waiting: 0
Calls that have been redirected while ringing: 0
Calls that have been redirected while waiting: 0
Calls where callers navigated to other destinations: 0
Total duration spent in IVR: 0:01:44
Total duration ringing: 0:02:10
Total duration talking: 0:41:38
Total duration holding calls: 0:01:32
Activity report of agents:
Agent Name
Availability
Calls
Duration
(Hold)
511 Jack Jacobs 0
513 Rachal Reed 3 0:24:56 0:00:31
514 Karla Miller 5 0:16:42 0:01:01

Figure 11-4. Summary of Agent Group Queue

The report also shows calls that are currently queued as well as information about each call, including source, destination, length of time the call has been in queue, and call state.

List of calls to the queue:

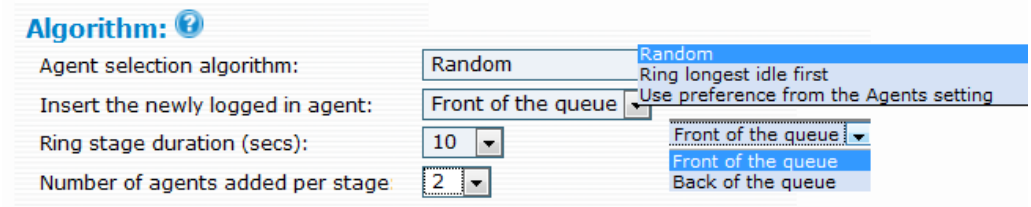
From	To	Time	Account	IVR	Ringi
snom ONE - PLEASANTON CA ((603)123-4567)	127.0.0.1 (unknown-dnis)	07:01:31		0:00:13	0:01:
((633)123-4567)	(978)746-2777	08:17:18	513	0:00:13	0:00:
((633)123-4567)	(978)746-2777	11:55:23		0:00:13	0:01:
snom ONE - PLEASANTON CA ((603)123-4567)	127.0.0.1 (unknown-dnis)	12:22:23	514	0:00:13	0:00:
snom ONE - PLEASANTON CA ((603)123-4567)	127.0.0.1 (unknown-dnis)	13:17:15		0:00:13	0:02:
snom ONE - PLEASANTON CA ((603)123-4567)	127.0.0.1 (unknown-dnis)	13:23:45		0:00:13	0:01:
(978)123-4567	(978)746-2777	14:51:33	514	0:00:13	0:00:
(978)123-4567	(978)746-2777	16:12:44	514	0:00:13	0:00:
(978)123-4567	(978)746-2777	17:03:41	514	0:00:13	0:00:
snom ONE - Unavailable (unknown-ani)	127.0.0.1 (unknown-dnis)	17:19:08	513	0:00:13	0:00:

Figure 11-5. List of Calls to the Queue

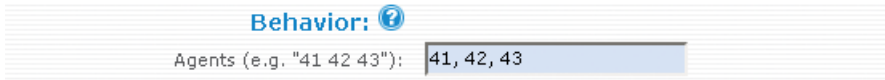
- **Record incoming calls to agent groups**: When this setting is enabled, the system will record all calls that come into the agent group. The recordings can later be retrieved and reviewed.
- **Automatically log out the agent if they missed the last call**: This setting will log out an agent who has missed a call. Agents need only log back in to return to the agent group.
- **Allow multiple ACD calls on agent - even if busy**: This setting allows a caller to be sent directly to an agent, even if all agents are busy. It prevents the caller from sitting there listening to music and gives the agent the opportunity to put their current call on hold and take the new call. This setting should generally not be used.

Connecting Caller to Agent

This section allows you to choose an algorithm for the system to follow when connecting a caller to an agent. When a caller needs to be connected to an agent, the system must determine which agent should be called next. There are currently three algorithms available to select from.



- **Agent selection algorithm**: The agent selection algorithm allows you to establish the method that will be used by the system when connecting a caller to an agent. Choose from the following options:
  - Random: This algorithm randomly selects the next agent. This is a reasonable algorithm in environments where it is not important as to which agent processes the call.
  - Ring longest idle first: This algorithm is designed to balance active call time amongst all the agents. The queue keeps a list of the agents and moves an agent to the end of the list when an agent connects a call. This ensures that the agent with the longest idle is at the front of the list.
  - Use preference from the Agent's setting: This algorithm uses the extensions listed in the Agent setting, as shown below (see **Behavior** settings on page 231). The agent listed first will be tried first. If that agent is busy, then the system will jump to the second one and so on.



- **Ring stage duration (secs)**: At regular intervals, the system checks agent availability and determines whether the next caller should be pulled out of the waiting state. The ring stage duration setting establishes this interval. For larger queues, shorter intervals are recommended, as it is quicker to get callers

out of the queue and into a ringback state. The default value for this setting is 5 seconds.

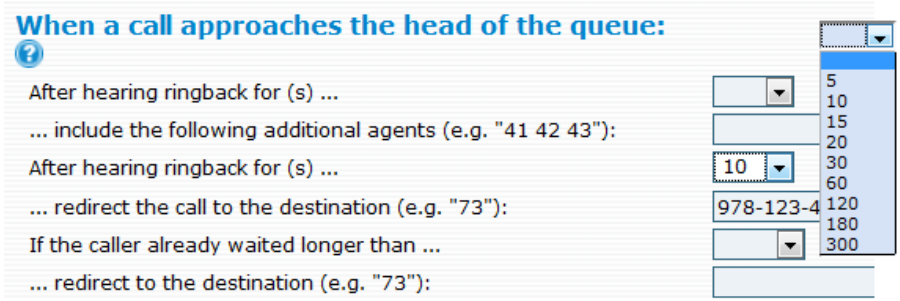
- **Number of agents added per stage**: In every scheduling interval, the system adds only a limited number of agents from its pool of available agents to its list of ringing agents. For large agent groups, a typical value would be one or two, as this will ensure that not all agents receive calls at the same time and so that the system CPU is not overtaxed with simultaneous calls. Figure 11-6 depicts one agent being added to the list of ringing agents every 10 seconds.

Figure 11-6. Ringing Agents at Fixed Intervals

Preventing Lengthy Periods in Ringback or Queue

Calls That Approach the Head of the Queue

This section allows you to establish timeout settings that will determine the length of time a call is kept in queue or ringback state in a given situation. In this section, you can instruct the system to add additional agents or to redirect a call after the call has been in ringback for a given length of time. You can also instruct the system to redirect a call once a caller's wait time has passed a certain threshold.



When configuring these settings, use the following table:

Table 11-2. Preventing Lengthy Periods in Ringback or Queue

After/If . . .	Then . . .	How/When to Use
After hearing ringback for (X) seconds,	include the following additional agents (e.g., 41 42).	Use this setting when additional people in the office can help out when no one else is picking up. **Result:** When calls are not picked up within the specified period, the system calls these extensions.
After hearing ringback for (X) seconds,	the system will redirect the call to the destination (e.g., 73).	The destination can be either an internal number (e.g., a hunt group) or an external number (e.g., a cell phone or home number). This option is similar to the previous option but instead of ringing both the original and new agents, the system cancels the original agents and redirects calls to the new agent(s) or to the external number. **Result:** After-hour callers are directed to a phone that will be picked up.
If the caller has already waited longer than (X) seconds,	the system will redirect the call to the destination (e.g., 73).	If a caller has waited a while in the queue, this will immediately redirect the call to another destination. *Note*: The caller is classified as "waiting" when all agents are busy with other customers and the new caller is waiting for a free agent. **Result:** If none of the agents free up within the specified period, the call will be redirected to the indicated number.

Mapping Telephone Keypad Numbers with Extensions

User Input Handling enables the caller to exit the agent group queue and connect to another destination. To give the caller this option, use the User Input Handling fields to map telephone keypad numbers to other extensions or phone numbers.

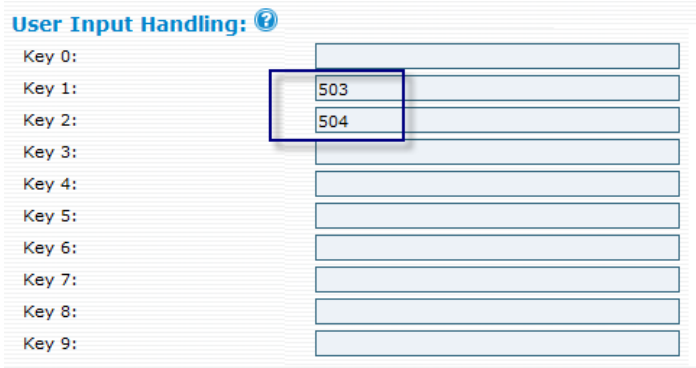


Figure 11-7. Mapping Keypad Numbers to Queue-Exiting Destinations

Once extensions or phone numbers have been entered into the "Key" fields shown in Figure 11-7, the caller needs to be made aware that these options are available. The system will not do this automatically. The place to do this is through the greetings that are delivered by the system (using the *98 star code feature). One greeting or several greetings can be used to inform the caller that this additional option is available. In Table 11-3, greetings 2 and 5 have been recorded to let the user know that keys 1 and 2 can be used to exit the agent group queue. (Figure 11-7 corresponds to the table. The user must press 1 to be redirected to 503 and 2 to go to 504.)

Table 11-3. Using Greetings for Agent Group Escape Routes

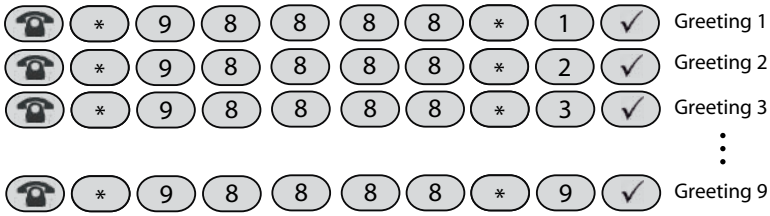
Greeting	Message	User Input Handling
0	Welcome to CompanyABC. Your call is important to us. Please hold.	
1	Sorry our lines are still busy . . . Have you looked at the support site for answer to your question?	
2	Our newest release offers this and that . . . If you want to leave a message, please press 1 now.	503
3	Another message . . .	
4	Another message . . .	
5	Another message . . . If you would like to leave a message, please press 2.	504

Recording Agent Group Greetings

The number of available greetings within any agent group is nine. Record only those greetings that should be used. If no greetings are needed, even an initial greeting, don't record any.

When recording greetings, you need to assign a number to each greeting; for example, *0 is the entry greeting, *1 is the first greeting, *2 is the second greeting, etc. The number is entered as the last number in the string.

1. Dial *98 followed by the number of the agent group, then the greeting number (e.g., *1).
2. Press the confirm button on the telephone keypad.



Listening to Greetings from the Phone

To listen to greetings quickly from the phone, change the gap between announcements to `1` and call the agent group directly from your phone. The recorded messages will be played quickly.

Night Service

Night service is used to redirect calls to other extensions or phone numbers during certain times of the day/night or other events that are outside normal business hours. Before night service can be used, a Service Flag account must be created for each night service number (see Chapter 8).

The first three settings in Night Service allow you to make provision for when no agents are available:

- **When primary agents are logged out, send calls to**
- **When call agents are logged out, send calls to**

- **When all agents are unregistered, send calls to**

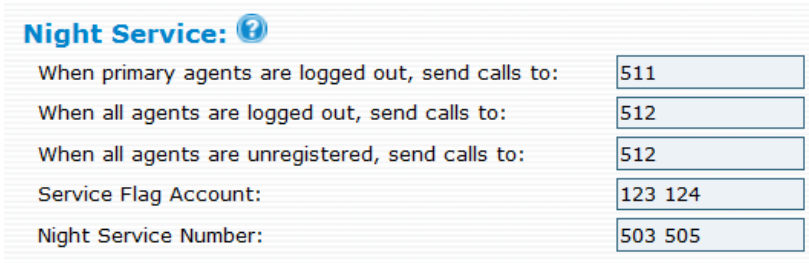
The following two settings are used to configure the service flag(s) to night service numbers:

- **Service Flag Account**: Once you have created the service flag account(s), enter the number of the account(s) into this field.

  Note: You may specify more than one night service flag (separated by a space). The first service flag account will correspond to the first night service number, and the second service flag account will correspond to the second night service number, etc.

- **Night Service Number**: Once a service flag is in place, calls will be directed to the night service number(s) indicated here. Internal extensions or external number phone numbers are permitted in this field.

  Note: You can also use a special character pattern (#L) to activate the service flag when all agents are logged out, even if the logout period is within normal working hours. All calls will automatically be redirected to the specified night service number(s).



SOAP Interface

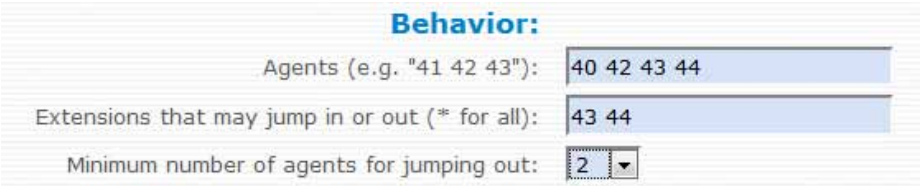
The SOAP interface allows you to use external logic to control the queue behavior. See Chapter 14 for a sample SOAP message.

- **Queue Status URL**: `http://www.snom.com/soap/pbx/queuestatus`

Logging In and Out

Agent group members can use one of two methods (buttons or star codes) when logging in and out of agent groups.

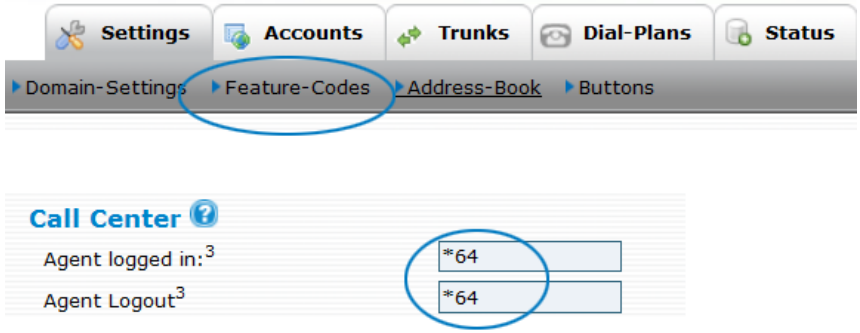
Important: Before agents can use either method, agents must be included in the **Extensions that may jump in or out** setting. Another setting that must be considered is the **Minimum number of agents for jumping out** setting (shown below). The latter setting is used to prevent the agent group from becoming too small; however, if this setting is too high, agents will be unable to log out of the agent group.


Behavior:
Agents (e.g. "41 42 43"):
40 42 43 44
Extensions that may jump in or out (* for all):
43 44
Minimum number of agents for jumping out:
2

Method 1: Buttons

This method allows users to use a button on their phone to log in and out of agent groups. When configured properly, the button will have a toggle effect. When the button is pressed, users will be logged in to all agent groups, and the associated LED(s) on their phone will light. When the button is pressed again, users will be logged out of all agent groups and the associated LED(s) will no longer be lit. If users need to log out of one agent group before logging into another, multiple **Agent login/logout** buttons can be configured. See page 330 for instructions on creating the button(s).

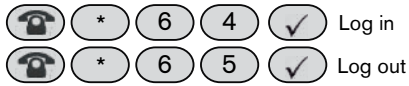
Important: Before you can use this button, the star codes for Agent logged in/Agent logged out must match (e.g., *64/*64).



Note: Agent group calls can be forwarded to an agent's cell phone. See **When calling the extension in an agent group** on page 468.

Method 2: Star Codes

When using star codes to log in and out of agent groups, users have the flexibility of logging in and out of all agent groups to which they belong or just a specific group. The standard **Agent logged in/Agent logged out** (*64/*65) star codes (without any argument) will log the agent in to or out of all agent groups:



Agents who are members of numerous agent groups and who need to log out of one agent group before logging into another can do so by entering the agent group number after the star code. Using the sample shown below, the agent will be logged out of agent group 666 and will retain logged-in status for all other agent groups.

Note: Agent group calls can be forwarded to an agent's cell phone. See **When calling the extension in an agent group** on page 468.

Monitoring Agent Groups

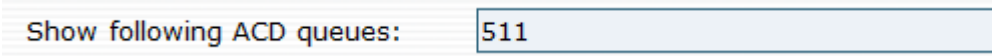
Agent groups can be monitored from the web interface through the buttons on the phone and from the WAC (Web-based Attendant Console). The method you use will be based on the type of monitoring necessary and the size of the domain and agent group. The different methods are detailed in the following sections.

Monitoring from the Web Interface

An agent group can be monitored from the user account or from the agent group itself.

To monitor from a user account:

1. Enter the agent group into the user's **Show following ACD queues** field.

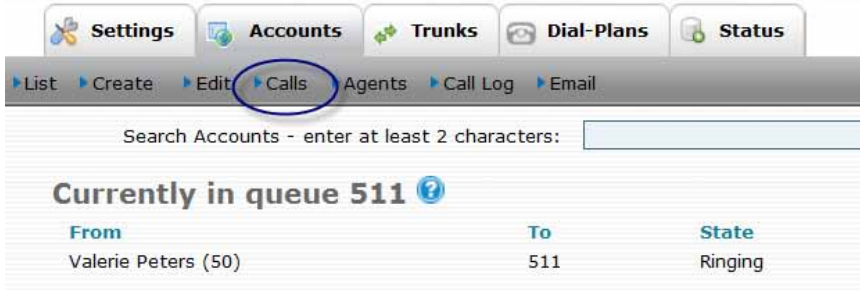


2. In the agent group itself, enter the extension into the **Queue Manager** field:

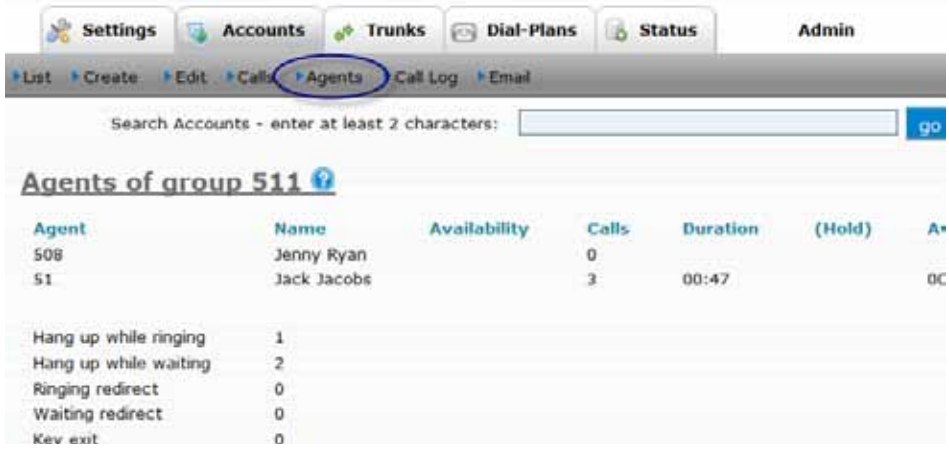
3. Log in as user and click the **Status** tab.
4. Click the agent group shown beneath the tabs.
5. Click **Calls** to see the active calls.
6. Click **Agents** to see which agents are on calls.

To monitor from the agent group account:

1. Open the agent group account.
2. Click **Calls** to view calls that are either ringing, in queue, or with an agent.

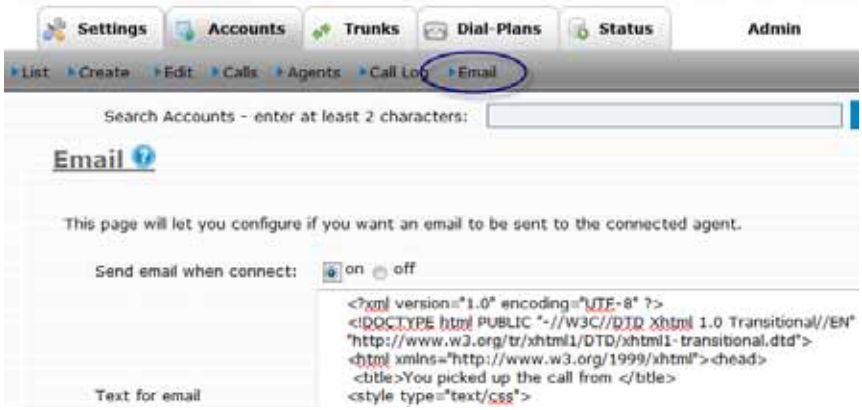


3. Click **Agents** to view agent-related information.



4. Click **Call Log** to view the call history of the agent group.

5. Click **Email** to send an email to a connected agent.



Monitoring Using Buttons on Phone

An agent group can be monitored through LEDs on the phone. To do this, create a button profile with Agent Group as the button type and the agent group number as the parameter. To monitor numerous agent groups from the phone, assign numerous buttons as Agent Group and enter the appropriate agent group into the corresponding parameter fields. When a caller is waiting in the group, the LED will blink fast. By pressing the button, you can pick up the call. A solid LED indicates that all calls have been picked up.

Name	Type	Parameter
	Not assigned	
1	Redirect	9781234567
2	Agent Group	73
3	Agent Group	74
4	Agent Group	75

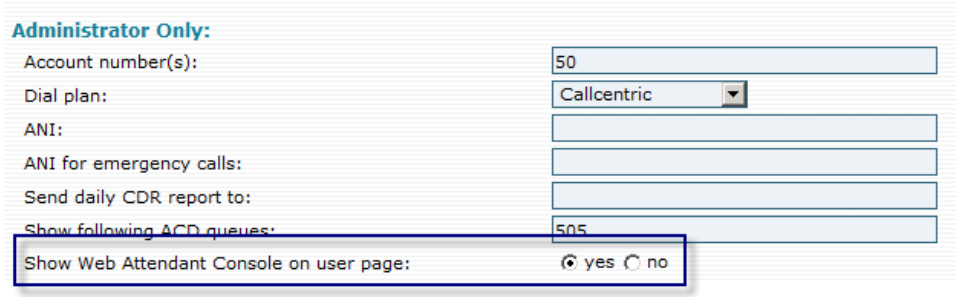
Monitoring from the WAC (Web-Based Console)

The WAC can be used to view the activities of the entire domain, including the status of agent group members. Agents are denoted by “AG” and a check mark. If your

domain is too large for all the extensions to fit on a single screen, the WAC may not display all the agents.

Users can access the WAC by logging into the web interface and going to **Status** > **WAC**.

This **WAC** link will be available only if the administrator has enabled the setting shown below (located in the user's account).



Users can also access the WAC by choosing **Console Login** from the **Login Type** drop-down when logging into the system.

Chapter 12

PAGING

Advanced IP phone systems allow even small offices to have a fully functioning paging system without using a standalone system. Paging can be thought of as a one-way audio session, as opposed to intercom's two-way audio. Paging allows a single extension to communicate with a few people (unicast paging) or a potentially large group of people (multicast paging). Users can page other users by dialing the paging account and speaking into the phone. Recipients will hear the message from the speaker on their phones. Several paging groups can be configured on the system so that different audiences can be addressed.

Types of Paging

Unicast Paging

Unicast paging is a one-to-one call to each participant in the paging group. The system establishes a regular call to each extension (Figure 12-1) through standard SIP calling. While this is usually fine for a small group, it can be burdensome for larger paging groups since it ties up a lot of resources in the system. A paging group with 20 extensions is essentially a 20-person conference call. Due to the increased demand on CPU performance, this unicast paging is appropriate for paging groups consisting of no more than ten extensions.

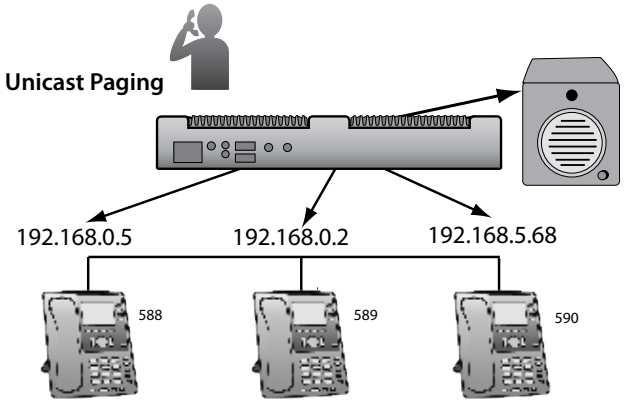
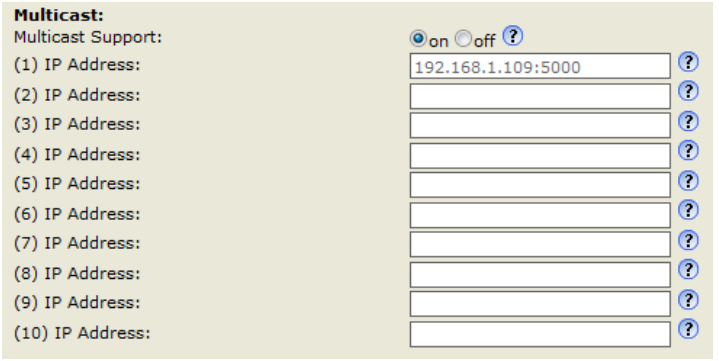


Figure 12-1. Unicast Paging

Multicast Paging

A multicast page is essentially a predefined broadcast address that phones or SIP user agents are programmed to listen to. Each phone can be configured to listen to as many as 10 different multicast IP addresses.



The advantage of a multicast page is that only *one* SIP session is established between the originator and the system (Figure 12-2). Subsequently, the system sends only one RTP stream to the multicast group on which the phones are listening. If 100 phones are listening on a multicast page, it is equivalent to a single phone call, instead of a 100-party conference call. This makes multicast paging suitable for groups that number in the thousands.

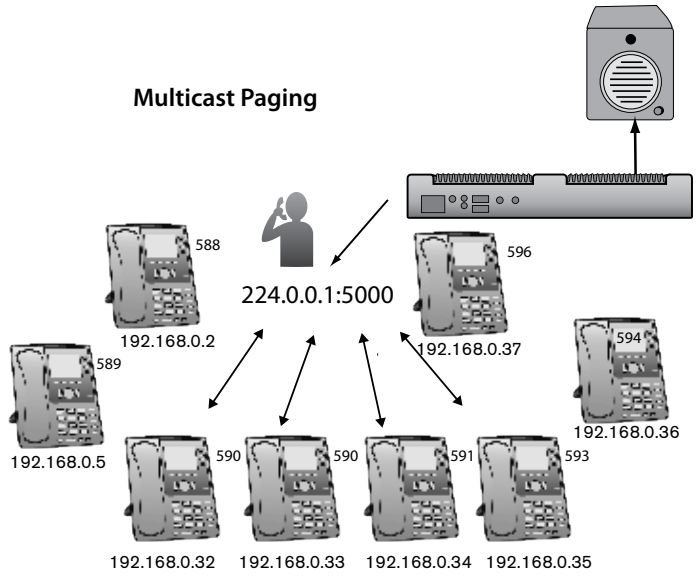
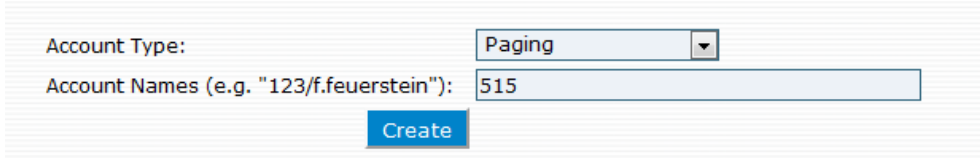


Figure 12-2. Multicast Paging

Setting up a Paging Account

This section provides instructions for creating and configuring a paging account on the snom ONE.

1. From the **Accounts** tab, click **Create** and select **Paging** from the dropdown:



2. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

```
515/9781234567
```

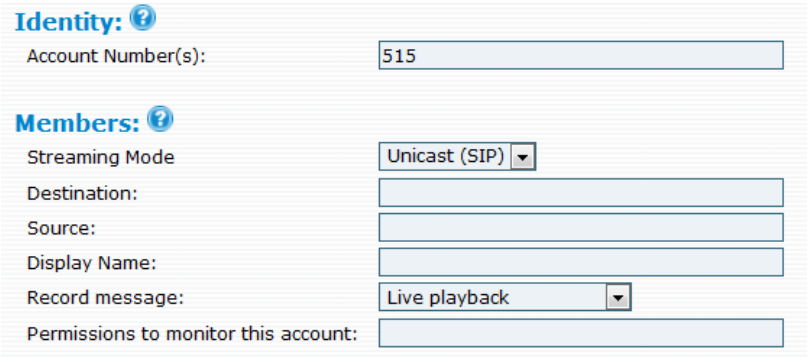
Note: If you use a space instead of a slash (`515 9781234567`), you will create two separate accounts that will be unrelated to each other.

Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts under accounts page at the domain level (**Domain** > **Settings**).

To create multiple accounts at the same time, use a space between the numbers:

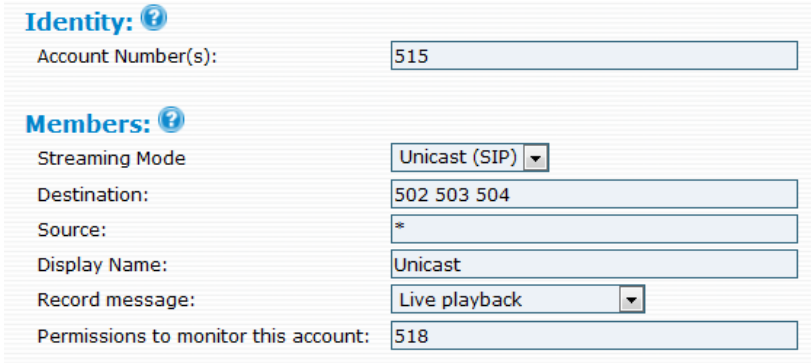
```
515 516 517
```

3. Click **Create**.
4. Once the account has been created, click **List** and open the account:

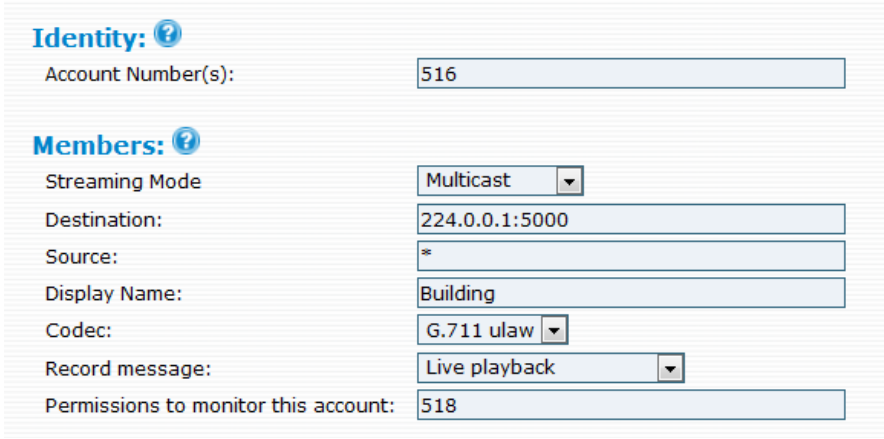


Configure the account as detailed below:

- **Account Number(s)**: This field takes extension number(s) and/or DID number(s). The number of DIDs that can be entered into this field is unlimited. This information can be changed at any time.
- **Streaming Mode**: This setting allows you to determine how your paging group will be set up:
  - **Unicast (SIP):** When using unicast mode, you'll need to provide a list of destination numbers for your paging group in the next setting (Destination). With unicast paging, the system initiates a call to all extensions listed, so be sure to limit your paging group to no more than 10 extensions. Unicast paging is not limited to the local area network, so all extensions that are connected to the system will be paged regardless of location.



– **Multicast:** Multicast mode allows you to designate a single IP address as your paging group and create paging groups that encompass entire organizations without taxing bandwidth (the end systems are unaware who the members of the multicast group are and do not send SIP signaling to the individual paging devices). When you page the group using this method, all devices configured to listen on the same multicast IP address will go into paging mode as soon as they receive RTP traffic on that port.



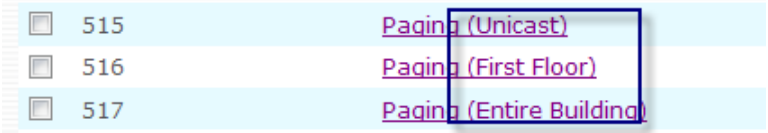
Not all phones support multicast paging. Phones that do have this support must be configured through the phone's web interface before they can be part of a multicast paging group (see "Assigning Multicast IP Addresses to IP Phones" on the next page).

- **Destination**: When using unicast mode, enter a group of extension numbers. When using multicast mode, enter an IP address.

  Note: When paging to IP phones, multicast addresses must range from 224.0.0.0 to 239.255.255.255. When using a traditional paging system, use the IP address (192.x.x.x) of the paging device.

- **Source**: List the extensions that are allowed to page this group. Enter a star (*) to give access to all extensions.

- **Display Name**: The display name will be used to identify the source of the call. SIP phones will display this text in the display area. The Accounts page will list the display name next to the account number:



- **Codec**: The system comes with G.711 and is free. Other codecs, such as G.729, require a fee due to the royalties associated with them.

- **Record message**: The **Record message** feature can operate in two different modes:

  - Live playback: This mode allows you to send a page in real time. With this mode, you pick up the phone, dial the paging account number, and start speaking/paging. All interested parties will hear the page.

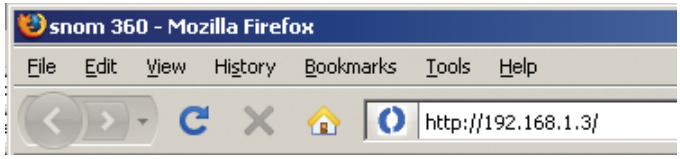
  - Play recorded message: This mode has a store-and-forward mechanism and requires that you record the message before sending it to the interested parties. With this mode, you pick up the phone, dial the paging account number, and start speaking. The system will record the message once you hang up and will send it to the interested parties.

- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this account.

Assigning Multicast IP Addresses to IP Phones

Before a phone can be part of a multicast paging group, a phone must have a multicast IP address that matches the snom ONE multicast IP address. This requires configuring the multicast settings for each phone.

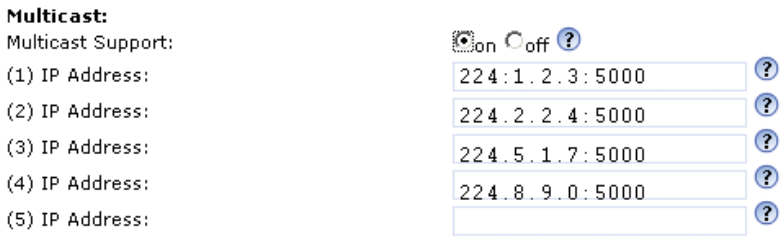
1. Go into the phone's web GUI by entering the phone's IP address into a web browser.



The following screen will appear:

2. Click **Advanced** at the left side of the screen.
3. Select **SIP/RTP** as shown below:

4. Scroll down to **Multicast** at the bottom of the page.



5. Enable **Multicast Support**.
6. Enter the IP address that was entered as the destination when configuring the multicast paging account in the web interface.
7. Click **Save**.

The phone can now pick up the RTP stream and begin playing it.

Chapter 13

CONFERENCING

A conference room or conference server is normally an expensive add-on with traditional phone systems. With the snom ONE telephone system, you can have your own conference rooms within your own system. Several types of conferencing can be used on the system: scheduled and ad hoc. The scheduled conference allows users to plan in advance for the conference and the ad hoc conference, as its name suggests, allows users to pull together a conference at a moment's notice.

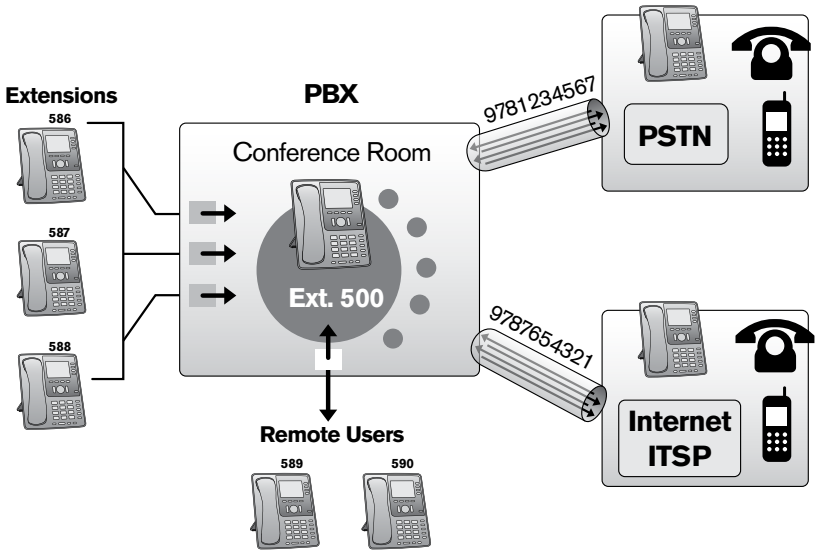


Figure 13-1. Conference Account Flow

Moderator settings can be configured from the web interface, and conferencing star codes can be used during the conference. Several conferences can be going on simulta-

neously in various conference rooms. All types of users (remote, snom ONE, PSTN) can call into both types of conferences.

Table 12-1 provides an overview of the conference features.

Table 13-1. Conference Account Features

Feature	Functionality	Benefit
Email notification	The system sends an email notification containing the time, date, conference room number, and purpose of the conference.	The conference organizer can notify participants easily, and users are notified in advance.
Outlook integration	Since email notification contains a calendar event, it can be read by Microsoft Outlook.	Users are unlikely to miss the conference.
Ad hoc conferences	Meetings can be established at a moment's notice by anyone inside or outside the office.	A manager can place a page announcing the details of a meeting, and everyone can call in.
PIN codes	PIN codes restrict admission to the conference. They are generated by the system and are included in the notification email that is sent to each invitee.	PIN codes add security. Only invited people can attend.
Moderator control	The conference leader receives an exclusive PIN code.	Moderator control allows the conference leader to receive the list of participants via email, execute star codes during the conference, and clear the conference when its over.
Conference recording	Conference leaders can record conferences. When participants enter the conference, they are informed that it will be recorded.	The conference leader can review the recording and email it. Everyone can have a personal copy of the conference.

Feature	Functionality	Benefit
Backdoor access	Rather than using valuable telephone lines for external conference attendees, inexpensive SIP trunks can be used.	SIP trunks significantly reduce the load on the main telephone lines and keep them open for customer use.
Multiple conference rooms	The system allows as many conference rooms as a license will permit. Each conference room has a unique number.	Conference rooms can be accessed from inside or outside the office. Different departments can conduct conferences at the same time.

Scheduled Conferences

The scheduled conference allows the conference leader to plan for a conference in advance. Users are informed via email of the time, date, and access code. The access code ensures that no unauthorized users can join the conference. Before users can schedule conferences, the administrator must set up at least one conference account. After the account has been created, users can schedule conferences by going to **Lists** > **Conferences** (available only from the user login). This section shows the administrator how to create the account itself.

Creating a Scheduled Conference Account

To create the conference account:

1. Click **Accounts** > **Create**.
2. Choose **Conference** from the dropdown.
3. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

   ```
   667/9781234567
   ```

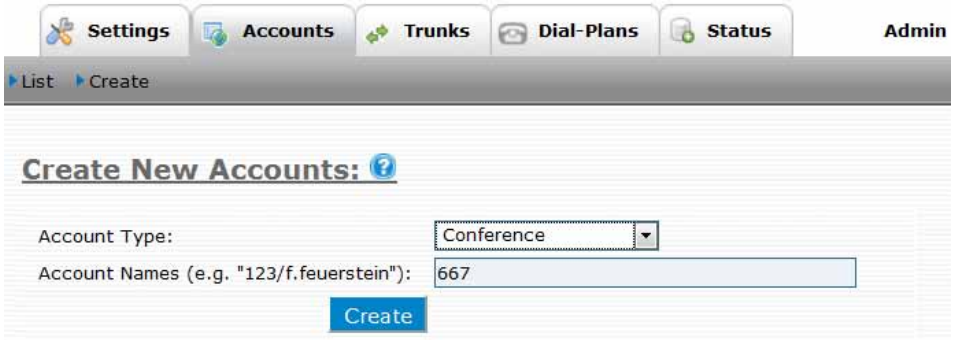
   Note: If you use a space instead of a slash (`667 9781234567`), you will create two separate accounts that will be unrelated to each other.

Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts under the accounts page at the domain level (**Domain** > **Settings**).

To create multiple accounts at the same time, use a space between the numbers:

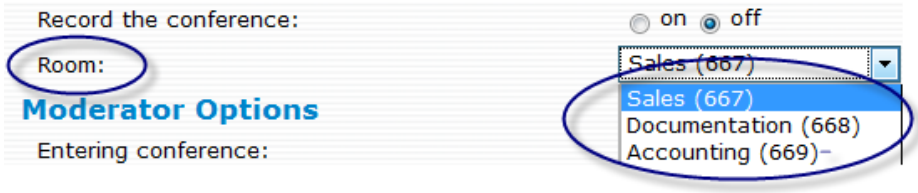
```
667 668 669
```

4. Click **Create**.

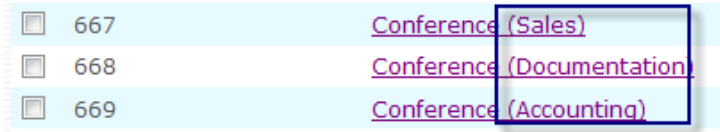


5. When the page reloads, click **List** to view the accounts, then click the edit icon to open the account. Most of the settings are self-explanatory, but keep the following in mind when populating the fields:

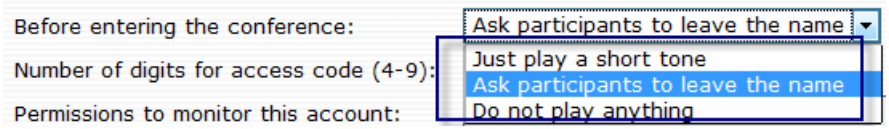
   - **Conference Name**: The name that is assigned to the conference will appear in the **Room** dropdown that is displayed on the page when the user goes to organize a conference. Choose a name that will help users differentiate one conference room from the next:



   The conference name will also be displayed next to the account number on the **Accounts** page:



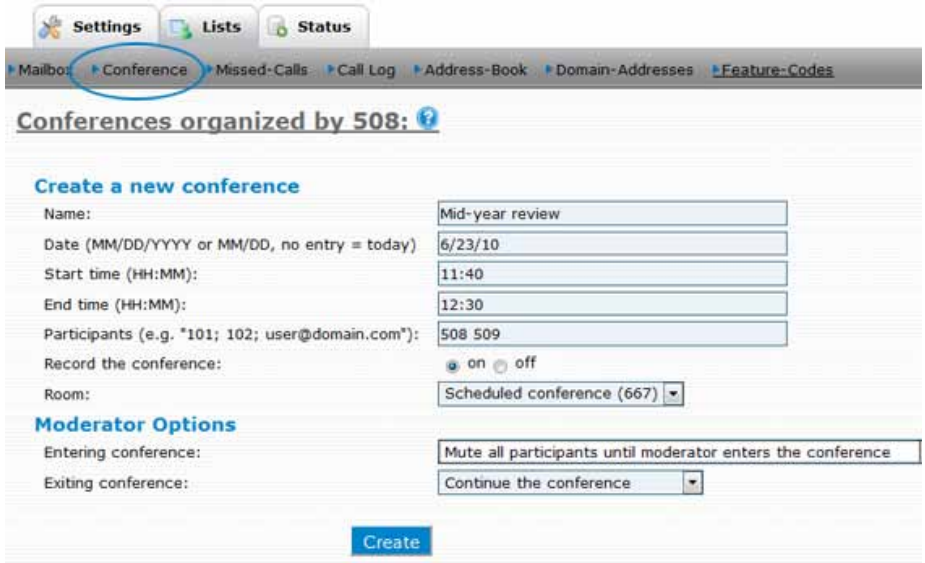
- **Mode**: Be sure to choose **Scheduled conference**.
- **Before entering conference**: The setting determines what occurs when the participant enters and exits the conference.


Before entering the conference:
Ask participants to leave the name
Number of digits for access code (4-9):
Just play a short tone
Ask participants to leave the name
Permissions to monitor this account:
Do not play anything

Scheduling a New Conference

Once a conference account has been created, users can create conferences from their own accounts:

1. Click **Conferences** from the **Lists** tab, as shown below:



2. Populate the form using the following information:
   - **Name**: This field allows participants to know the subject of the conference.
   - **Date**: Use `MM/DD/YYYY` (month/day/year) or `MM/DD` (month/day) format. Leaving this field blank will automatically schedule your conference for the day you populate the form.

- **Start and end times**: Use `HH:MM` (hours/minutes) format.

  Note: The system will use the selected time zone of the extension that is logged in. The start and end times must be in the same format.

- **Participants**: Enter extension numbers and/or email addresses. (The user's domain must be set up for sending out emails.) When listing multiple email addresses, use a **semicolons** as a space separator.

  The email contains a calendar event, which can be read by most scheduling tools. The tool will pop up a conference reminder with the relevant conference information.

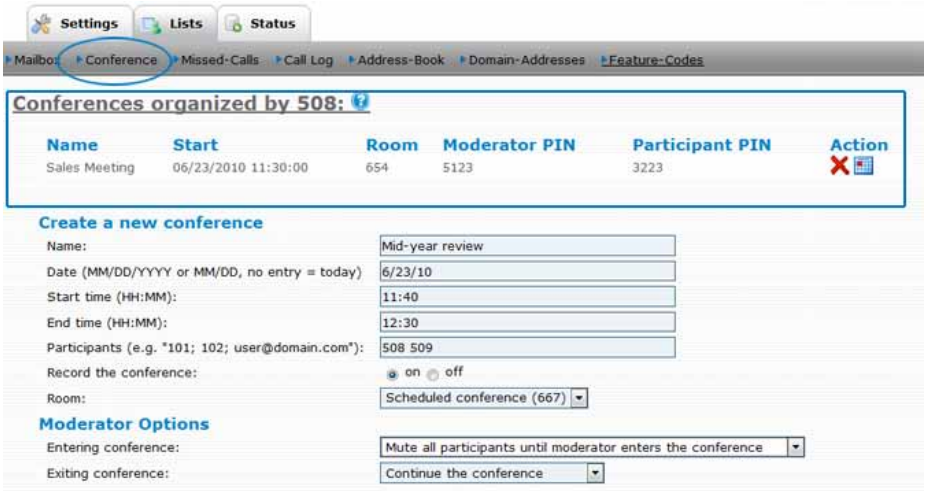
- **Record the conference**: The recording will be placed into the user's mailbox on the web interface (**Lists** > **Mailbox**).

- **Room**: Choose a conference room.

- **Moderator options**: These settings are discussed on page 265.

3. Click **Create**.

The new conference will be displayed under **Conferences organized**, listing the moderator and participant PINs. Participants will receive an email that includes conference details, such as date, time, and PIN number.

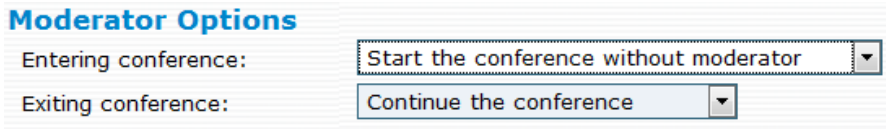


Modifying Scheduled Conferences

Once a conference has been created, it cannot be modified; it can only be deleted (click the delete icon in the conference list). Conferences are automatically deleted 24 hours after the conference end time; however, participants who want to continue talking before the conference is deleted can do so as long as the moderator specified **Continue the conference** as an exiting preference.

Moderating Scheduled Conferences

Web interface settings and star codes can be used to control a scheduled conference. The web interface settings are located in **Moderator Options** in the conference account:



These settings are described below:

- **Entering conference**
  - Start the conference without moderator: Participants will be able to communicate with each other upon entering the conference.
  - Mute all participants until moderator enters the conference: Participants won't be able to communicate with each other until the moderator calls into the conference.
  - Mute all participants until moderator unmutes the conference: Participants won't be able to communicate with each other until the moderator unmutes the conference (*8).
- **Exiting conference**
  - Continue the conference: Participants will be able to communicate with one another after the moderator has exited the conference. (The conference will not be deleted until after 24 hours.)
  - Mute all participants on exit: Once the moderator exits, participants' phones will be muted.

– Hang up the conference on exit: Once the moderator exits, the system will disconnect all participants from the conference call.

Table 13-2. Conference Star Codes

Star Code	Description
*0	Send participant list
*1	Mute your device
*2	Unmute your device
*7	Mute other participants[1]
*8	Unmute other participants[1]
*9	Hang up the conference[1]

1. Requires moderator privilege.

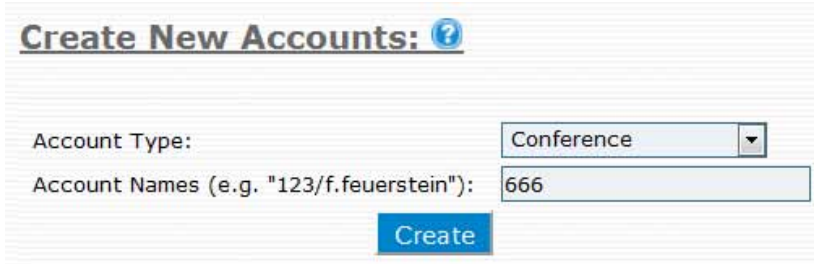
Note: As with the other conference star codes, *0 (send participant list) must be executed during the conference. A participants list will immediately be sent to the moderator via email.

Ad Hoc Conferences

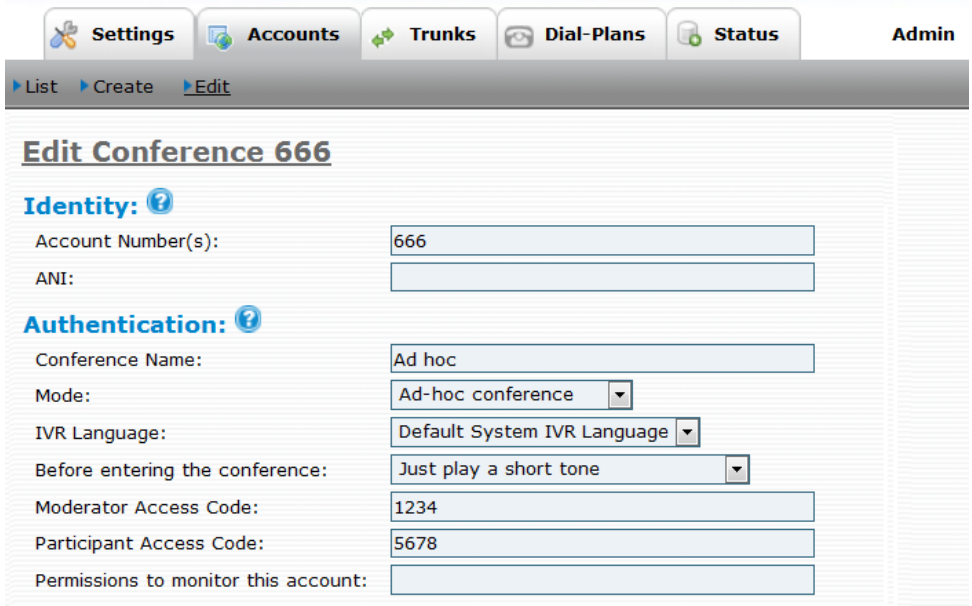
The ad hoc conference account allows users to hold conferences at a moment's notice. No planning is required, and no emails are sent out. This method of conferencing is handled through the system and produces a high-quality three-way conference. Although this method offers an especially simple way to hold a conference, unauthorized users will be able to access the conference room if an access code requirement has not been set on the account.

Creating an Ad Hoc Conference Account

1. From the **Accounts** tab, click **Create** and select **Conference** from the drop-down.



2. Enter the extension number and a name that will be associated with the account, then click **Create**.
3. Once the account has been created, click **List** to open the account and configure it as detailed below:



- **Account Number:** You can change the name of your conference or the extension number of your account at any time.
- **ANI**: The conference account uses an ANI (automatic number identification) when sending calls to an external number.

- **Conference Name**: It is recommended that you choose an understandable name for the conference, e.g., `Company A conference mixer (2106171234 Ext 654)`, as this text will be used in conference invitation emails.
- **Mode**: Select **Ad-hoc conference**.
- **IVR Language**: From the dropdown list, choose the language that will be used for the voice responses.
- **Moderator Access Code**: This field can be left blank; however, the conference cannot be moderated without an access code (see "Moderating an Ad Hoc Conference" on page 245).
- **Participant Access Code**: When no moderator access code has been set, this field can be left blank; otherwise, a code is required (users will be unable to access the conference without a code if the moderator has one).
- **Permissions to monitor this account**: Enter the extension numbers of the individuals who are permitted to monitor this account.

4. Click **Save**.

Calling into an Ad Hoc Conference

To hold an ad hoc conference, users need to know the extension number that has been reserved for ad hoc conferencing. If the designated extension is 665, then all parties who enter 665 from their extension phones will be joined to the same call. Participants will be required to enter an access code if one has been set; otherwise, they will be joined directly into the conference room. Any number of participants can join the call. (Participants can also be blind-transferred into the conference.)

Moderating an Ad Hoc Conference

Moderators can use the following star codes to dynamically control an ad hoc conference. If no moderator access code has been set, these star codes will not function.

Table 13-3. Conference Star Codes

Star Code	Description
*0	Send the participants list
*1	Mute your device
*2	Unmute your device
*7	Mute all
*8	Unmute all
*9	Hang up the conference

Note: As with other conference star codes, *0 (send participant list) must be executed during the conference. An email listing the participants will immediately be sent to the moderator.

Chapter 14

IVR NODE

At the most basic level, the interactive voice response (IVR) system allows callers to reach their destination by making touch-tone entries through the phone keypad, rather than going through the operator. An IVR node can also be configured for complex tasks so that callers can enter account numbers and pay bills through an external application server.

Note: The IVR node and auto attendant are two distinct accounts. Auto attendants with basic functionality (routing callers from point A to B) do not need an IVR node and can use the built-in IVR that is available through the auto attendant account (see Chapter 9 for more information). Table 14-1 lists the IVR node features:

Table 14-1. IVR Node Features

Feature	Functionality	Benefit
Caller verification	Callers are required to enter their account number when reaching an IVR.	Caller verification expedites service to legitimate callers and prevents undesired callers from wasting employees' time.
Password call routing	Callers are required to enter their password before getting routed to the correct destination.	Password call-routing provides an automated means of controlling the flow of information to the appropriate contacts.
Auto fax detection	Upon detecting a calling signal from a fax, the system answers the call and sends it to your fax machine.	A dedicated fax line/number is no longer needed to receive faxes.

Feature	Functionality	Benefit
Response-based routing	Response-based routing uses caller input to route a call to the person or information best suited to assist. The system asks the caller a question, and the caller responds by entering a digit.	By developing a series of questions to which the caller can respond, the system can effectively route the caller. Response-based routing saves time and the expense of an interviewer.
Expedited caller-ID routing	Incoming calls that match a number currently on an IVR list are automatically routed to a pre-defined destination.	Employees working outside the office can be connected to the correct department by dialing the main number. Preferred customers can be routed based on their caller-ID. Unwanted callers can be routed to "dead ends" or busy signals to discourage them from calling.
Announcement before ringing	The system greets every caller with a uniform message prior to connecting the call: Example: "Thanks for calling XYZ Sales. Please have your account code ready." "Thanks for calling Pizza King. Be sure to ask about today's special."	Information can be delivered before the caller is connected. This prepares the caller, expedites call flow, and makes your initial greeting count.

How the IVR Node Works

When a caller reaches an IVR node, the system plays back the prompt that has been set for that IVR node. Once the caller answers the system by pressing the required digit(s), the system will continue processing the call. This first IVR node is typically used as an entry door into the system, and the nodes that follow are used to decide how to proceed next with the caller. For example, the IVR node can ask the customer for account

information then ask an external application server where the customer should go from there. Based on the answer from the external application server, the customer is routed to the appropriate waiting queue.

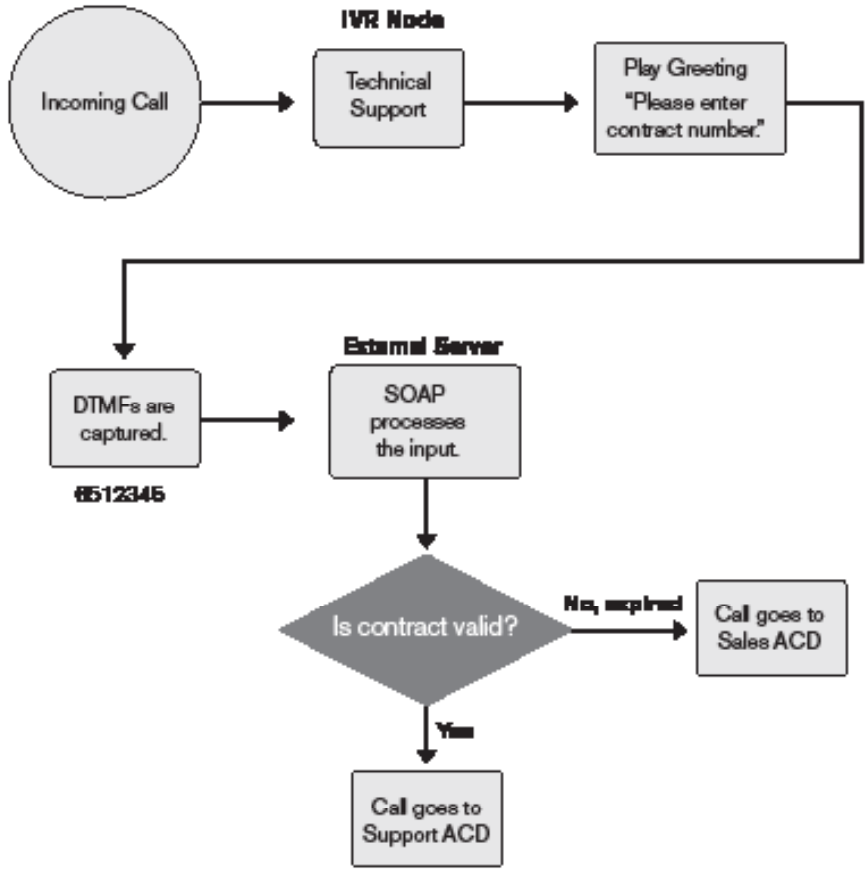


Figure 14-1. IVR Node—User Enters Contract Information

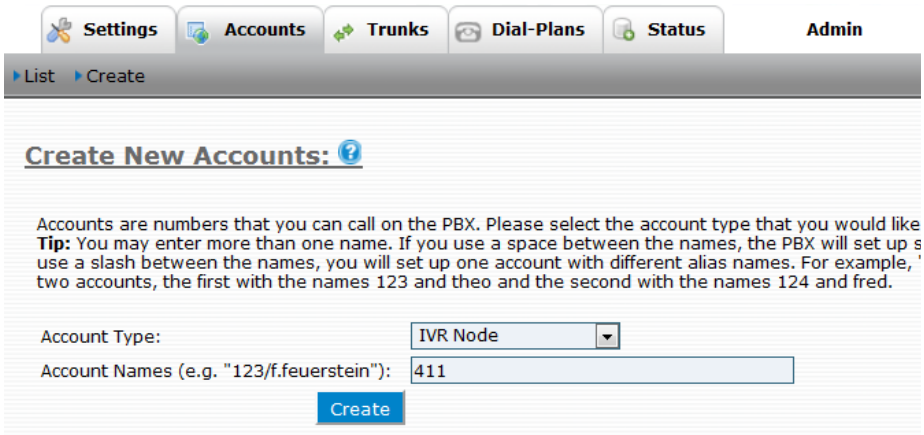
An IVR node can also be used to define dialog that will be used to process calls. In this case, each node plays one prompt and asks a specific question to the caller. The first prompt may ask the caller what language is preferred and then dispatch the caller into two different node systems for two different languages. This IVR node mechanism is very flexible and allows you to either process the input internally in the system or use an external application server to decide where to go next. The IVR node collects the user input according to the list of ERE expressions that was entered in the node's match list.

In the simplest case, a static routing is sufficient without consulting the external server, but it depends on the user input.

Setting up an IVR Node Account

This section provides instructions for creating and configuring an IVR node on the snom ONE.

1. From the **Accounts** tab, click **Create** and select **IVR Node** from the dropdown:


Settings
Accounts
Trunks
Dial-Plans
Status
Admin
List
Create
Create New Accounts:
Accounts are numbers that you can call on the PBX. Please select the account type that you would like
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up s
use a slash between the names, you will set up one account with different alias names. For example,
two accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
IVR Node
Account Names (e.g. "123/f.feuerstein"):
411
Create

2. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

```
411/9781234567
```

Note: If you use a space instead of a slash (`411 9781234567`), you will create two separate accounts that will be unrelated to each other.

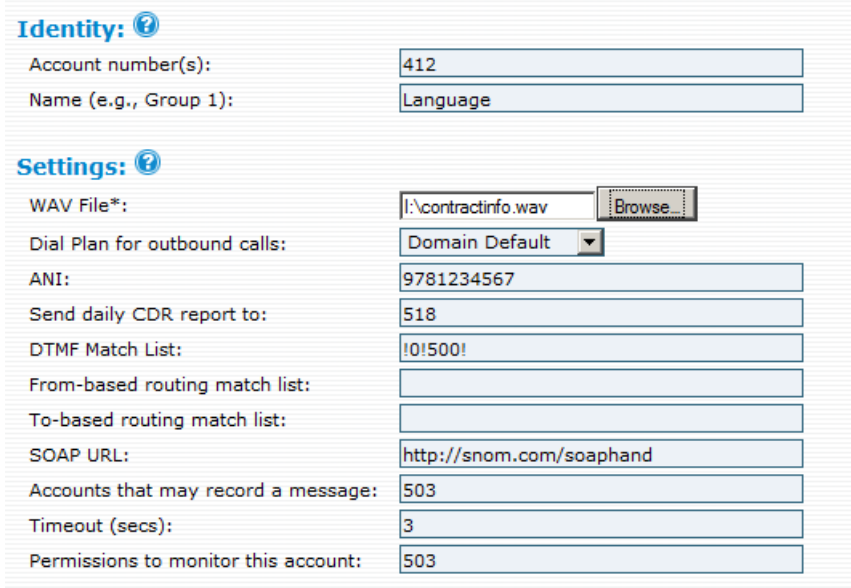
Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide aliased accounts under the accounts page at the domain level (**Domain** > **Settings**).

To create multiple accounts at the same time, use a space between the numbers:

```
411 412 413
```

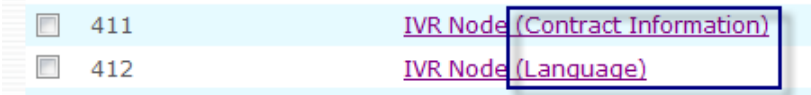
3. Click **Create**.

4. Once the page reloads, click **List**.
5. Click the account to open it.
6. Configure the account as described in the following sections:



Identity

- **Account Number(s)**: This field takes an extension number(s) and/or DID number(s). The number of DIDs that can be entered into this field is unlimited.
- **Name**: This field allows you to create an alias so that you can quickly distinguish the IVR nodes from one another.



Settings

- **WAV File**: An external recorded announcement can be uploaded in wave format (8-kHz Mono, 16-bit files). Announcements can also be recorded by dialing *98888, where 888 is the IVR node account.
- **Dial Plan for outbound calls**: Choose the dial plan that you would like the system to use when routing calls to an outside provider.
- **ANI**: The IVR node uses an ANI (automatic number identification) when sending calls to an external number.
- **Send daily CDR report to**: The call data record (CDR) lists all calls that come into the IVR node. The report is sent at midnight each night to the email address specified here.
- **DTMF Match List**: This field allows you to enter a list of match patterns that will be used by the system to direct a call once a user has pressed a number from the telephone keypad. You can also use pre-coded IVR nodes (see page 205 for information on direct destinations).

  When entering DTMF match patterns, keep the following criteria in mind:

  – A space is required between list elements.

  – Each pattern must contain two fields separated by a character that does not occur anywhere else in the string, for example "!".

  – The first field must contain the extended regular expression, and the second field must contain the destination.

  Example: To specify that the caller should be directed to extension 500 after pressing 0, enter `!0!500!` into the DTMF field. To specify that the system should wait until a user has entered three digits before attempting to redirect the call, enter `!^([0-9]{3})$!\1!`.
- **From-based routing match list**: This field requires syntax similar to the DTMF field.
- **To-based routing match list**: This field is used when the snom ONE opens the IVR node. Use the same format as in **DTMF Match List** above. If there is a match with the `From` or the `To` header of the call, then the IVR node im-

mediately switches the destination without playing the WAV file. This allows you to implement flexible routing schemes.

- **SOAP URL**: If no SOAP URL is specified in the account, the system will assume that the matching pattern is the name of the account to switch to. If the SOAP URL is available, it will pass the destination to the application to further determine what to do with it. For more information on SOAP, see page 279).
- **Accounts that may record a message**: Enter the extensions that are allowed to record welcome messages. Use a star (*) to indicate all users.
- **Timeout (secs)**: The timeout specified in this field starts either when the system sends the call to the IVR node or when the user enters a digit.
- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this account. The destination may be any dialable number. If the number requires a dial plan, the default dial plan of the domain will be used. If the destination field contains a single dash ("-") and the pattern matches, the system will disconnect the call.

Recording Messages

Messages can be recorded using the Record Message (*98) star code, or they can be uploaded through the web interface. Both methods are detailed in the following sections. Users must have permission to record greetings before they can record greetings for an IVR node using *98. The permission is given in the IVR account itself.

Record the Message Directly

To record the message:

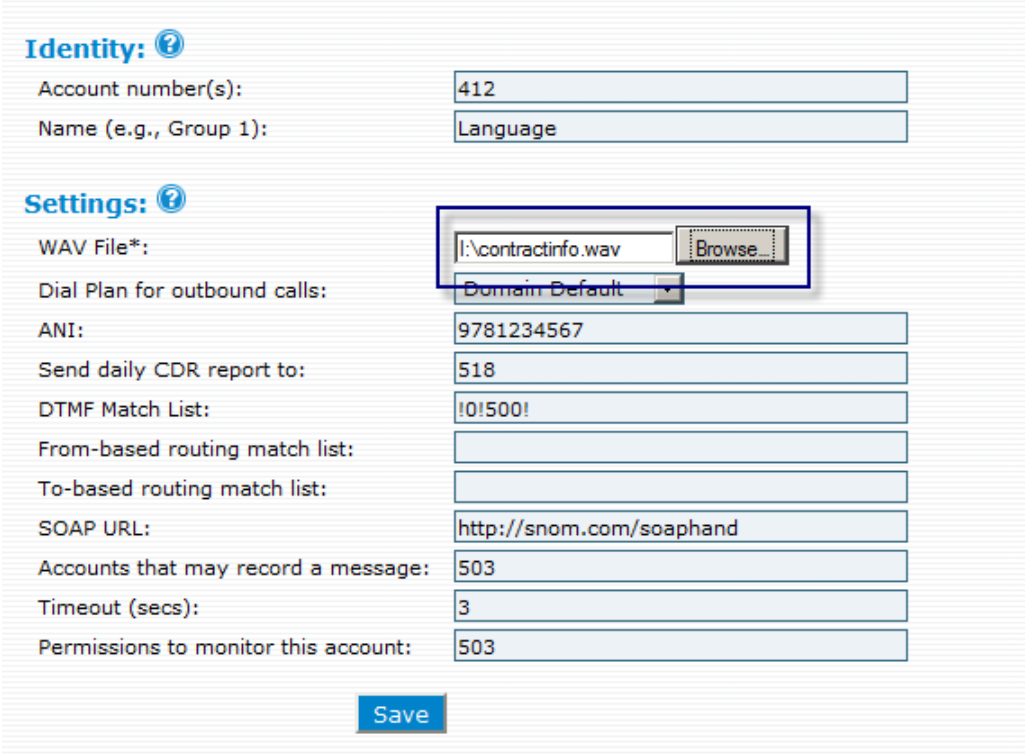
1. From the telephone keypad, enter *98.
2. Enter the IVR Node account number.
3. Enter *1 ("1" is the greeting number).
4. Press the confirm button.

In the example shown above, the IVR node account is "126," and the greeting that is being recorded is greeting 1. You may record up to nine greetings. The standard greeting is recognized by the system as greeting 0 and can be recorded by entering *98. Use the standard greeting if you want to use the same greeting for all hours of the day and night.

Upload a WAV File

WAV files allow you to record and edit your message before loading it into the system. They also allow you to use professional IVR dialogs. From the IVR Node settings:

1. Click the **Browse** button and upload the file (WAV files should be 8 kHz Mono, 16 bit).
2. Click **Save**.



Linking an External Application Server to an IVR Node

SOAP (Simple Object Access Protocol) is an XML message-based protocol specification used to allow applications running on a decentralized, distributed environment to exchange information. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other application layer protocols, such as RPT and HTTP, for message negotiation and transmission.

Sample SOAP Message

Following is a sample data interchange using the HTTP/SOAP protocol. (The indentation shown is for illustration purposes only.)

Request

```
POST /ivr.xml HTTP/1.1
Host: pbx.com
SOAPAction: IvrInput
Content-Type: application/xml
Content-Length: 123
<env:Envelope
    xmlns:env=" http://schemas.xmlsoap.org/soap/enve-
lope/"
    xmlns:sns=" http://www.snomone.com/soap/pbx">
  <env:Body>
    <sns:IVRInput>
      <CallID>3525234@snomone.com</CallID>
      <Output>123</Output>
      <From>Fred Feuerstein &lt;sip:ff@test.com&gt;</
From>
      <To>Tom Test &lt;sip:tt@test.com&gt;</To>
    </sns:IVRInput>
  </env:Body>
</env:Envelope>
```

In the snomone namespace, the record CDR indicates that a CDR shall be transmitted. The CDR may have the following attributes:

- `CallID`: This attribute contains the call-ID of the call and makes it possible to put the IVR input into a session context. It is also used as an identifier in the response to the request.
- `Output`: The digits that the user has entered into the IVR node.
- The `To` and `From` fields indicate the To and From headers of the call.

Response

The response on the file tells what should be done with the input. An example return could look like the following:

```
HTTP/1.1 200 Ok
Content-Type: application/xml
Content-Length: 123
<env:Envelope
    xmlns:env="http://schemas.xmlsoap.org/soap/enve-
lope/"
    xmlns:sns="http://www.snomone.com/soap/pbx ">
  <env:Body>
    <sns:IVROutput>
      <CallID>3525234@snomone.com</CallID>
      <Destination>123</Destination >
    </sns:IVROutput >
  </env:Body>
</env:Envelope>
```

The response has the following attributes:

- `CallID`: This attribute contains the caller-ID of the call. It is used to identify the affected call.
- `Destination`: This string indicates which account to switch to.

Example PHP File

This example shows how to process the CDR on an Apache web server using the PHP extension. This example just extracts the data and writes it into a plain file.

```
<?php
$elem="";
$callid="";
$output="";
function start_element($parser, $name, $attrs) {
  global $elem;
  $elem=$name;
}
function end_element($parser, $name) {
}
function xml_data($parser, $data) {
  global $elem, $from_user, $to_user, $from, $to, $du-
ration, $start, $callid, $output;
  if($elem=="CALLID") $callid .= $data;
  else if($elem=="OUTPUT") $output .= $data;
}
$content = $HTTP_RAW_POST_DATA;
$xml_parser = xml_parser_create();
xml_set_element_handler($xml_parser, "start_element",
"end_element");
xml_set_character_data_handler($xml_parser, "xml_
data");
if(!xml_parse($xml_parser, $content, true)) {
die(sprintf("Get XML error parsing %s: %s at line %d",
            htmlspecialchars($content),
            xml_error_string(xml_get_error_code($xml_
parser)),
            xml_get_current_line_number($xml_pars-
er)));
}
xml_parser_free($xml_parser);
```

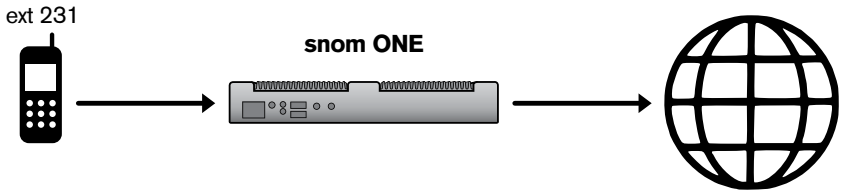
```
// Ok here some bogus logic what to do with the input:
$result = "123";

$xml = '<env:Envelope xmlns:env=" http://schemas.xml-
soap.org/soap/envelope/ " xmlns:sns=" http://www.sno-
mone.com/soap/pbx">';
$xml .= '<env:Body><sns:IVROutput><CallID>';
$xml .= $callid;
$xml .= '</CallID><Destination>';
$xml .= $result;
$xml .= "</Destination></sns:IVROutput></env:Body></
env:Envelope>\r\n";
echo $xml;
?>
```

Chapter
15

CALLING CARD ACCOUNT

The calling card account allows callers to place outbound calls from the system without being logged into their extension. This is especially advantageous to the user who is traveling. To place an international call, users simply call into the system and enter their extension number and PIN code. The call will reflect the office's caller-ID and will appear in the user's call log.



The calling card account can be used in three different modes:

- DISA —The user calls into the account and authenticates himself by entering his extension number and the associated PIN code. If the user's company has an 0800 number, then this is a simple away to reduce costs for international calls.
- Callback—The user calls into the system and requests a callback. Although this mode requires more steps to establish the call, it may reduce telephone costs even further, as the call to the system does not get connected and the caller is not charged for the call. When callback is initiated from the calling card account, rather than the Personal Virtual Assistant, the user will not be charged for the seconds/minutes that accumulate between the time the callback is initiated and the caller is connected to the destination.
- Pre-pay—The user calls into the auto attendant from an outside phone and enters his extension number and PIN. Once the system completes the au-

thorization, the user enters the destination number. The minutes accumulate against the user's **Credit for outbound calls** setting (see page 171).

The calling card account can also be used with an external database. Customers who buy a prepaid calling call can dial into a free-of-charge number that goes into the calling card account. The system uses the SOAP interface to communicate with an external application server which manages the calling cards and the remaining money. Once the call has ended, the system reports the call duration to the server.

Setting up a Calling Card Account

This section provides instructions for creating and configuring a calling card account:

1. From the **Accounts** tab, click **Create** and select **Calling Card**:

Settings
Accounts
Trunks
Dial-Plans
Status
List
Create
Create New Accounts:
Accounts are numbers that you can call on the PBX. Please select the account type that you would like to crea
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up several a
use a slash between the names, you will set up one account with different alias names. For example, "123/the
two accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
Calling Card
Account Names (e.g. "123/f.feuerstein"):
103

2. In the **Account Name** field, enter an extension number and/or alias, i.e., a DID number. When entering an alias in addition to an extension number, use the following syntax:

```
103/9781234567
```

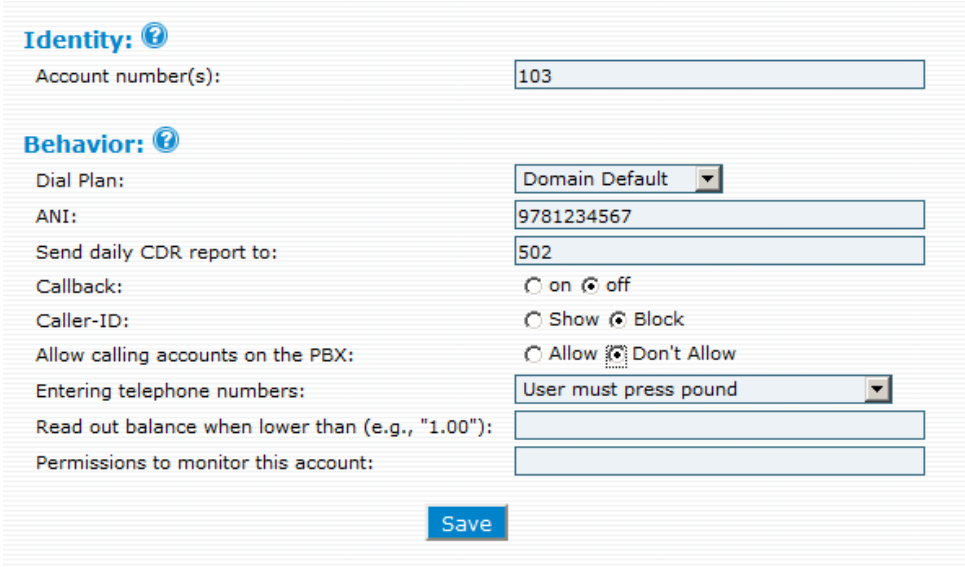
Note: If you use a space instead of a slash (`103 9781234567`), you will create two separate accounts that will be unrelated to each other.

Alias accounts can give the impression that your system has more accounts than it actually has and can clutter it up. If this occurs, you can hide the aliased accounts under the accounts page at the domain level (see page 101).

To create multiple accounts at the same time, use a space between the numbers:

```
103 104 105
```

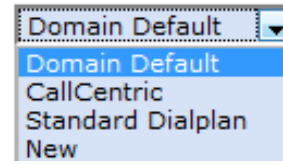
3. Click **Create**.
4. Once the page reloads, click **List**, open the account, and configure it as described in the following sections.



Identity

- **Account Number(s)**: This field takes extension number(s) and/or DID number(s). The number of DIDs that can be entered into this field is unlimited. This information can be changed at any time.

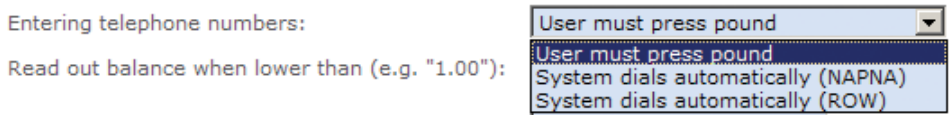
Behavior



- **Dial Plan**: Choose the dial plan that you would like the system to use when routing calls to an outside provider. If the system uses the SOAP interface for placing outbound calls, it needs to know which dial plan to use. If the system uses the internal database, it uses the dial plan of the selected extension.
- **ANI**: When a dial plan is used, the system also checks the presence of an ANI (automatic number identification) number and, if set, the system will use it.
- **Send daily CDR report to**: The call data record (CDR) lists all calls originating from the calling card account. The report is sent at midnight each night to the email address specified here.
- **Callback**: This feature allows the account to be used in callback mode. After dialing into the system, the user is prompted to enter an extension number and PIN code. The caller may leave a callback number; otherwise, the system will use the caller-ID. Once the system calls back, a destination number will be requested. The callback feature allows users to make free outbound calls from a cell phone as long as the cellular provider offers free incoming calls and the user has an unlimited call plan with one of the system's trunks.

  Important: Before users can use the calling card in pre-paid mode, **Callback** must be set to **off** (refer to Chapter 16 for information on the pre-pay feature).
- **Caller-ID**: Choose whether to show or block the caller-ID. If you choose to show the caller-ID and a call is started on behalf of a known extension, the system will use the caller-ID associated with that extension. If the SOAP interface is being used, the system will display the caller-ID of the calling card account.
- **Allow calling accounts on the PBX**: When this setting is enabled, the system will also consider calling local accounts. This is often useful in corporate environment, where callers can use 0800 numbers to call internal destinations.

- **Entering telephone numbers**: The system needs to know how to interpret a user's input. Choose from the options shown in the dropdown (a description of each option is listed below):

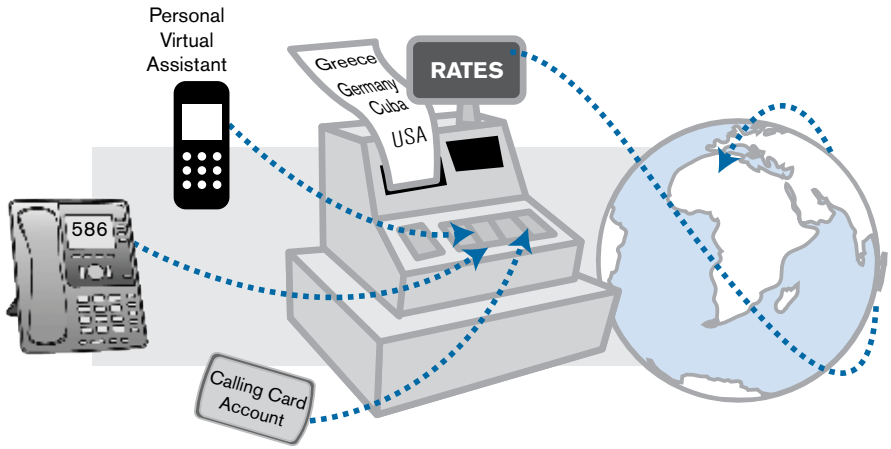

Entering telephone numbers:
Read out balance when lower than (e.g. "1.00"):
User must press pound
User must press pound
System dials automatically (NAPNA)
System dials automatically (ROW)

  - User must press pound: The user will be required to press the pound key after entering the telephone number.
  - System dials automatically (NANPA): The system will interpret telephone numbers according to the NANPA scheme (North American Numbering Plan Administration), which means that international numbers will start with 011 and numbers that have 10 digits will be written in the (xxx)xxx-xxxx scheme (see Table 3-2 for more information on NANPA).
  - System dials automatically (ROW): The system will interpret numbers according to a "rest of world" scheme, which means that international numbers start with 00 and national numbers start with 0 (see Table 3-2 for more information on ROW).
- **Read out balance when lower than (e.g., "1.00")**: The system will let the user know when the card balance is lower than the amount that is indicated in this field.
- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this account.

Chapter
16

PRE-PAY FEATURE

The pre-pay feature allows the administrator to create customized rate tables for multiple pricing strategies. Calls are calculated based on call duration, destination, and the rates provided in the tables. The pre-pay feature can be configured so that users can access it using the extension account, the Personal Virtual Assistant (available from the cell phone), or the calling card account (PIN access).



Users do not need a physical phone connection in order to take advantage of the prepay feature. This feature can also be accessed through a calling card account (see Chapter 15).

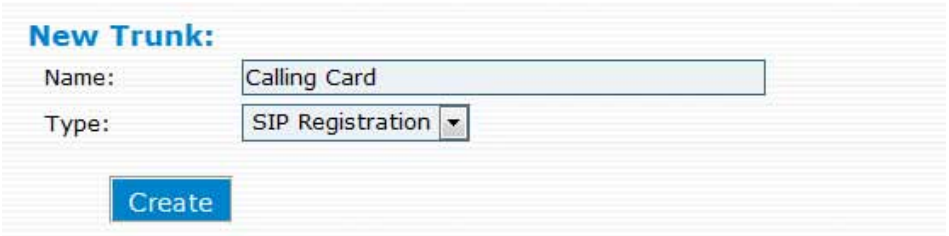
Setting up the Pre-Pay

The two important components of the pre-pay are the rates table and an assigned dollar amount on the user's extension:

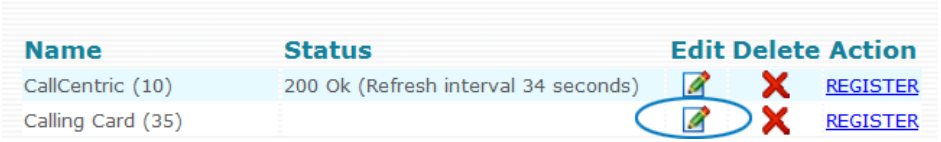
- Rates table—A rates table, CSV (comma separated value) formatted data, is an essential component to the pre-paid feature. It can include any number of entries and must be entered into the trunk.
- Dollar amount—A dollar amount must be assigned to the user's extension account.

Creating the Rates Table

1. Create a trunk that will be used specifically for the pre-pay feature.

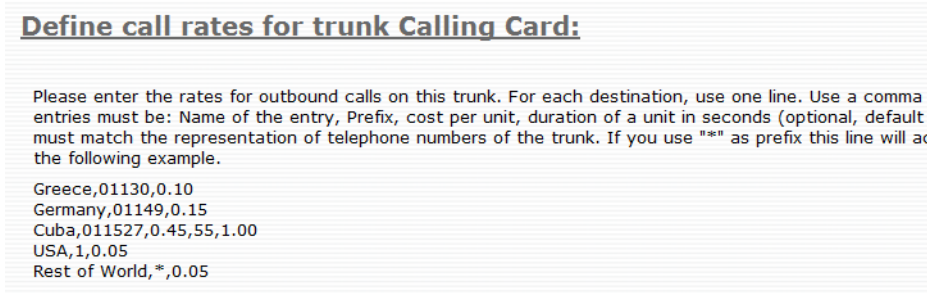


2. Click **List** to view a list of the trunks
3. Click the **Edit** icon for the trunk you just created:



4. Click **Rates**.

A sample rates table is displayed:


Define call rates for trunk Calling Card:
Please enter the rates for outbound calls on this trunk. For each destination, use one line. Use a comma
entries must be: Name of the entry, Prefix, cost per unit, duration of a unit in seconds (optional, default
must match the representation of telephone numbers of the trunk. If you use "*" as prefix this line will ac
the following example.
Greece,01130,0.10
Germany,01149,0.15
Cuba,011527,0.45,55,1.00
USA,1,0.05
Rest of World,*,0.05

The rates table follows standard CSV format. All fields are separated by commas:

```
Greece,01130,0.10
Germany,01149,0.15
Cuba,011527,0.45,55,1.00
USA,1,0.05
Rest of World,*,0.05
```

Following is a tabular representation of this information. As the table shows, different telephone area codes and exchanges will be charged at different rates.

Name of Entry	Prefix**	Cost per Unit	Duration of Unit (seconds)*	Connection Fee
Greece	01130	0.10		
Germany	01149	0.15		
Cuba	011527	45	55	1.00
USA	1	0.05		
Rest of World	*	0.05		

* The Duration of Unit default is 60 seconds.

** When establishing the prefix, the following settings must be considered: **Country Code** and **Area Code settings** (page 94) and **Rewrite global numbers** (page 140).

5. Enter your own calling rates in the space under the sample rates table.

   Important: In the event a blank field sits between two other fields (e.g., you're requiring a connection fee but will not be changing the Duration of Unit default, as shown in the table below), you will need to make provision for this empty space in your CSV syntax. CSV syntax in this case would be `Greece,01130,0.10,,1.00` (notice the double commas).

Name of Entry	Prefix	Cost per Unit	Duration of Unit (seconds)*	Connection Fee
Greece	01130	0.10		1.00

   All other trunk settings are detailed in Chapter 4.

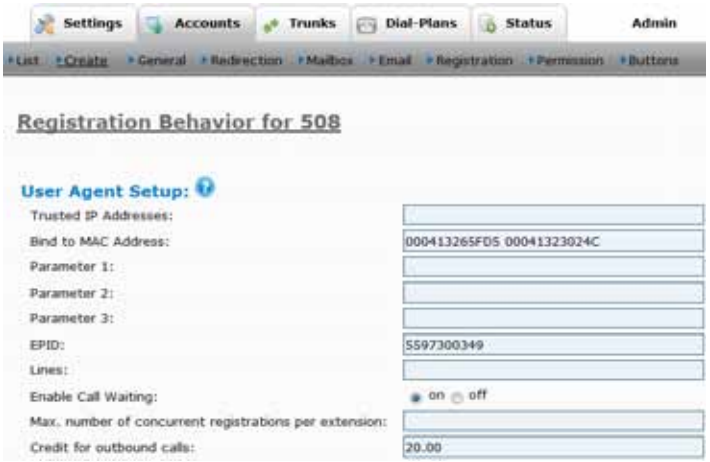
Assigning a Dollar Amount to an Extension

Before a user can begin using the pre-pay calling card account, a dollar amount must be specified in the extension account:

1. Open the user's extension, and click the **Registrations** tab.
2. In the **Credit for outbound calls** setting, enter a dollar amount.

   Important: If this field is left blank, the user will be allowed unlimited calling.

   Note: Users can execute the Show Account Balance (*61) star code to determine the number of minutes that are left on the pre-paid account.



Methods of Access

The pre-pay feature can be accessed via the extension, the Personal Virtual Assistant, or the calling card. This section details each method.

Extension

This method does not require a calling card. Once the rates table has been added to the trunk and the extension has been assigned a dollar amount, all calls made from the extension will be calculated according to the rates table assigned to the trunk. To determine the number of minutes remaining on the account, the user can execute the Show Account Balance (*61) feature.

Personal Virtual Assistant

With this method, users can call into the Personal Virtual Assistant from their cell phone to access their pre-paid account (the cell phone must be configured to the user's account). Instructions are as follows:

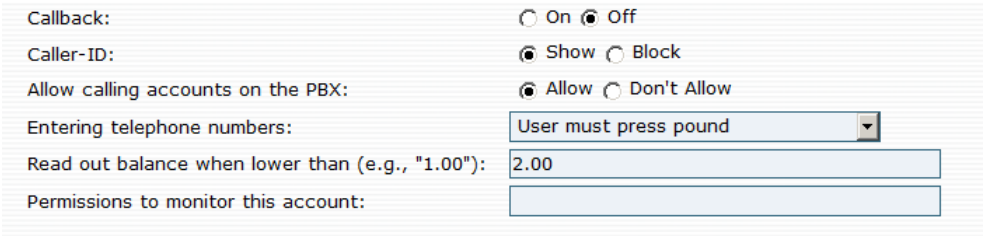
1. Call into the main number from the cell phone. Because the cell phone is recognized by the system, the user is presented with the Personal Virtual Assistant.
2. From the Personal Virtual Assistant, press 1 (to make an outbound call).
3. Enter the destination number.

   As with the previous method, the call will be calculated according to the rates table assigned to the trunk. To determine the number of minutes remaining on the account, the user can execute the Show Account Balance (*61) feature.

   The Personal Virtual Assistant is discussed on page 451.

Calling Card Account (PIN Access)

This method requires a calling card account. (Once you have created the account, be sure to deactivate the **Callback** setting and specify an amount for the **Read out balance** setting.)



This method will require that the user enter a PIN number for each call that is made.

Important: For security purposes, always require that your users enter a PIN. Do not try to configure the calling card account so that a PIN is not required.

To use the calling card account:

1. Call into the auto attendant from an outside phone.
2. Enter the calling card account number.
3. Enter the extension number.
4. Enter the PIN of the extension.
5. Enter the destination number.

   The call will be calculated according to the rates table assigned to the trunk. The system will read out the minutes remaining once the **Read out balance** threshold has been reached on the account. To get a readout of remaining minutes before the threshold has been reached, users can execute the Show Account Balance (*61) feature.

Chapter 17

EMAIL

E-mail support is one of the most useful and powerful features of the snom ONE telephone system for both the administrator and the user. The system can be configured to notify the administrator (or anyone else in charge) when calls get rejected, when the system disconnects a call, or even when someone dials an emergency number. Many other critical system events can also be included in this alert.

Users, too, can be notified of important events on their end. They can receive emails when they miss a call, at the end of every call, or whenever a call is rejected due to blacklisting. Users can also configure their account so that voicemails are sent as email attachments. This configuration enables them to check their voicemails at any time from any location in the world using an Internet connection.

This chapter shows the administrator how to configure these settings, as well as how to configure the SMTP server on snom ONE.

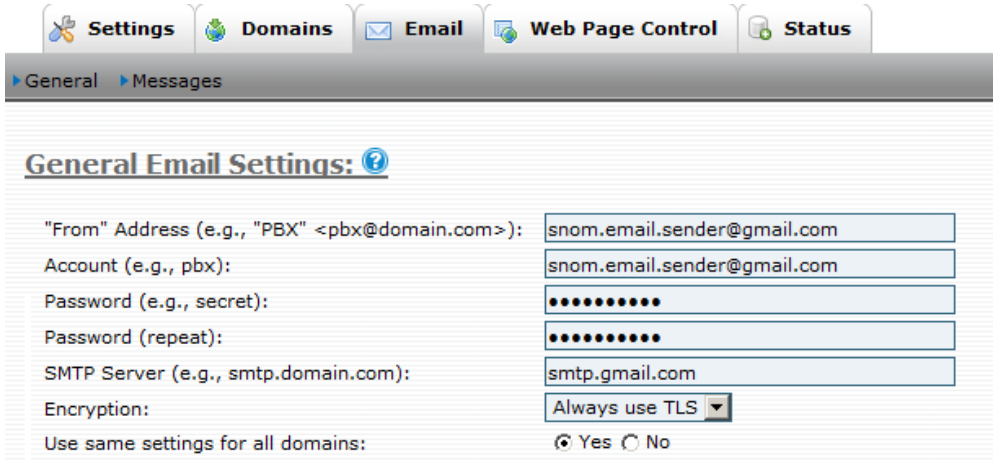
Configuring the SMTP Server

System-Wide SMTP Settings

The snom ONE telephone system can be configured as an email client to send email messages to the users. To do this, the system needs a mail or an SMTP server (via an external SMTP provider) to send the messages. If you already have an SMTP server set up, you can configure it to the system using the following instructions. If you do not have one set up, you can set one up through Gmail for free or ask your email administrator.

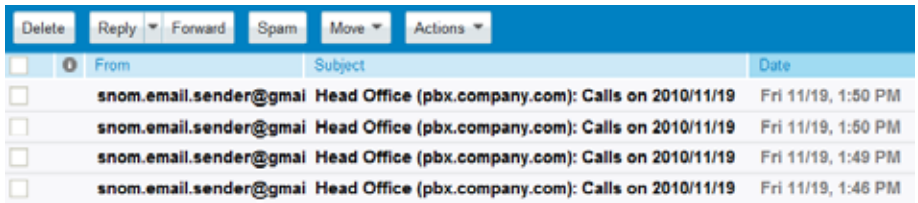
Note: SMTP settings can be configured by either the administrator or the domain administrator.

1. Navigate to **Admin** > **Email**:



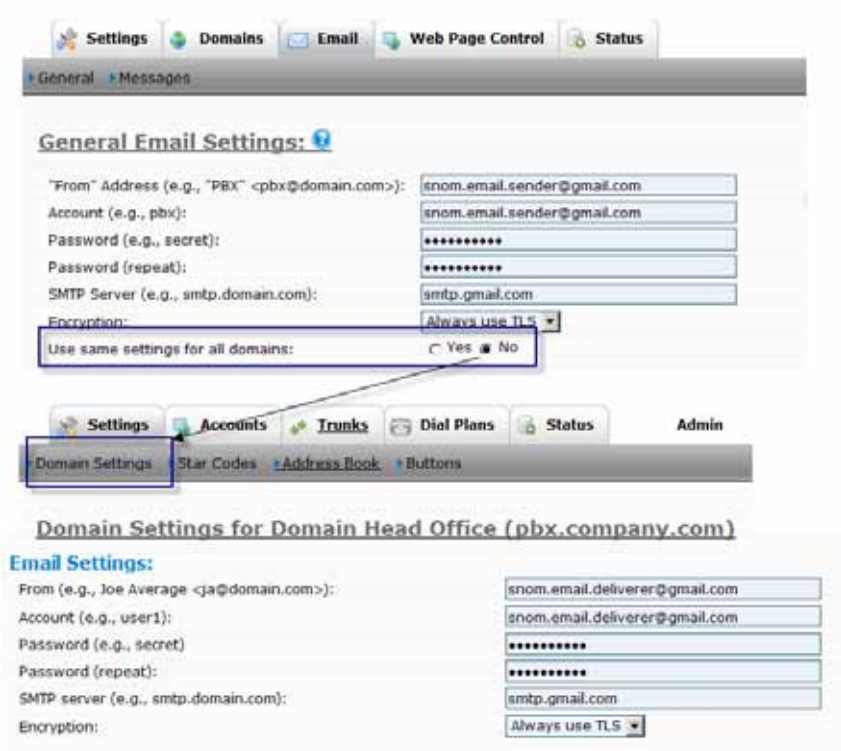
2. Populate the form using the following information:

   - **From Address:** This field will be used by the system when it sends emails. You can use names like `voicemail@your-company.com` or `pbxau-tomailer@your-company.com`. The name will appear in the `From` field of the email, as shown below:


Delete
Reply
Forward
Spam
Move
Actions
From
Subject
Date
snom.email.sender@gmai Head Office (pbx.company.com): Calls on 2010/11/19 Fri 11/19, 1:50 PM
snom.email.sender@gmai Head Office (pbx.company.com): Calls on 2010/11/19 Fri 11/19, 1:50 PM
snom.email.sender@gmai Head Office (pbx.company.com): Calls on 2010/11/19 Fri 11/19, 1:49 PM
snom.email.sender@gmai Head Office (pbx.company.com): Calls on 2010/11/19 Fri 11/19, 1:46 PM

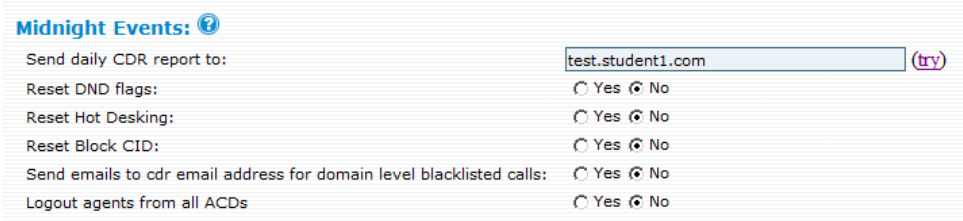
   - **Account:** Provide the e-mail account for the SMTP server. Generally, this is the same as the `From` address.
   - **Password:** This is the password for the e-mail account.
   - **Password(repeat):** Confirmation for the password.
   - **SMTP Server:** This is your SMTP outgoing mail server. The system can send email messages by emulating an email client; however, it needs a mail or SMTP server to send the messages. If you are using Gmail's SMTP server (`smtp.gmail.com`), you will need to add a certificate (see page 298 for instructions on setting this up).

- **Encryption:** This setting allows you to activate/deactivate TLS.
  - Automatic: If the email server needs TLS, then the system will start TLS, otherwise, TLS will not be considered. Basically, there is a negotiation process before sending the email.
  - Don't Use TLS: If you know that your mail server does not support TLS, use this setting.
  - Always Use: If your mail server requires TLS, then use this setting (gmail requires TLS).
- **Use same settings for all domains:** When this setting is set to **`Yes`**, all domains share the same SMTP settings. If this setting is set to **`No`**, each domain is permitted to configure its own SMTP settings (i.e., email settings are displayed in the **Domain Settings** tab within each domain, as shown below).

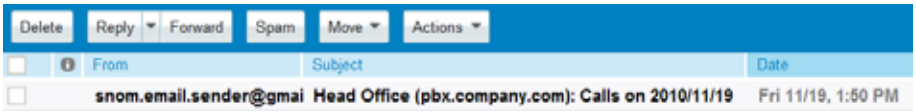


3. Click **Save**.

4. To test your email configuration, go to **Domains** > **Settings**.
5. Scroll toward the bottom of the page to Midnight Events.



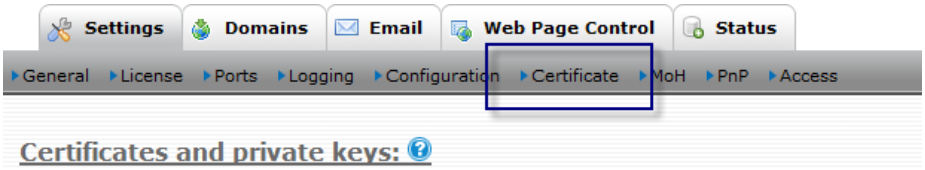
6. Enter a valid email address into the field shown above, and click **try**. You will receive an email from the system:



Certificate for Gmail SMTP Server

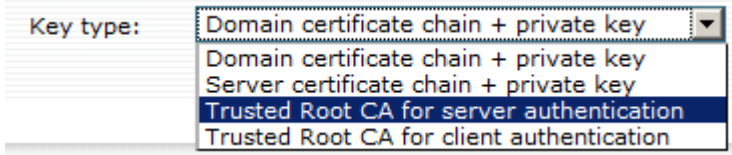
Certificates can be obtained from wiki.snomone.com. Once you copy the necessary certificate onto your clipboard, proceed as follows:

1. Go to **Admin** > **Settings** > **Certificate**.



2. Enter the certificate information into the **Certificate** field:

3. From the **Key type** dropdown, select **Trusted root CA for server authentication**.


Key type:
Domain certificate chain + private key
Domain certificate chain + private key
Server certificate chain + private key
Trusted Root CA for server authentication
Trusted Root CA for client authentication

4. Click **Save**.
5. To test your email configuration, go to **Domains** > **Settings** and click **try** from the **Send daily CDR report to** setting.

Adding Email Accounts to the System

Note: First create your email accounts using Gmail, Yahoo, or another webmail service provider. Once you have created your email accounts, you can add them to your extensions by clicking the **Email** link in each extension account (Figure 17-1) and then entering the email address into the **Email Address** field. When entering multiple email addresses, use a semicolon as a field separator.

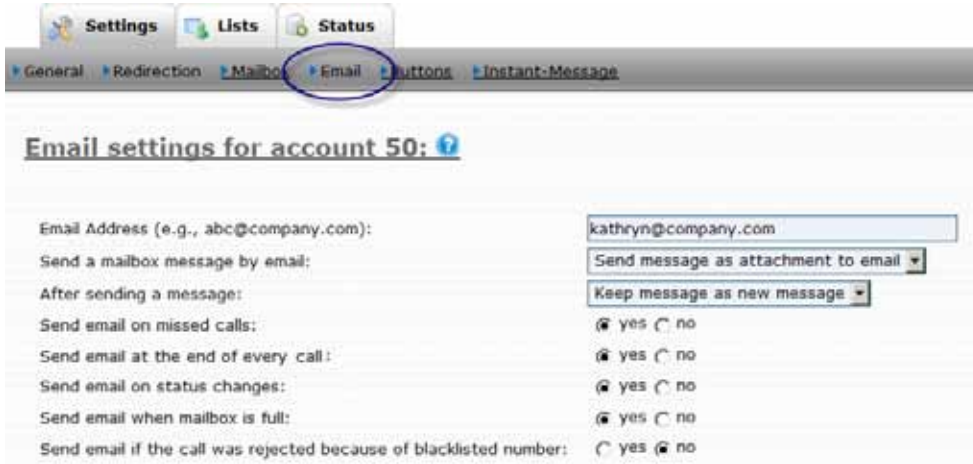
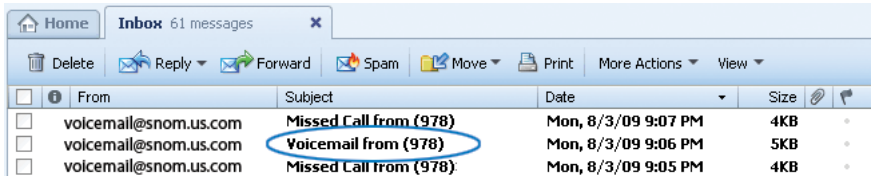


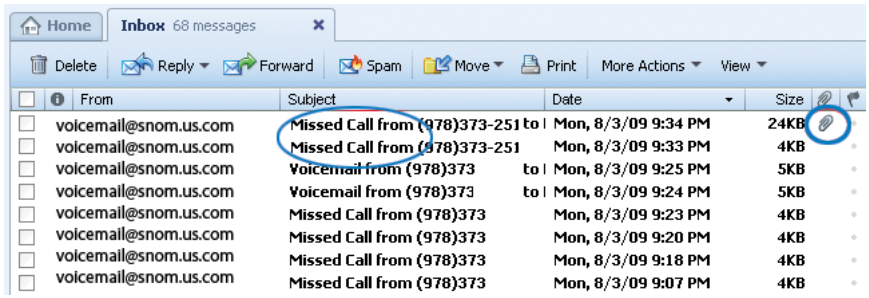
Figure 17-1. User Email Settings

Note: Figure 17-1 shows the standard email settings that are available to the user, but administrators can prevent the user from seeing the **Send a mailbox message** and **After sending a message** settings (see the email control settings on page 81).

- **Send a mailbox message by email**: Users have the following three options:
  - **Do not send an email**: No email will be sent. Only the extension will receive messages.
  - **Send emails without attachments**: Email notifications will be sent to the user whenever a voicemail message is received. This provides somewhat of a visual voicemail box. The email will show the name and number of the caller and the date and time that the call arrived. To retrieve the voicemail itself, the user will need to call into the voicemail. The benefit of this mode is that emails that are relatively short can easily be read using mobile devices that support reading emails.



  - **Send message as attachment:** Actual voicemails will be attached to the email notifications. This option is suitable for users who use email throughout the day and are using a personal computer for processing email.

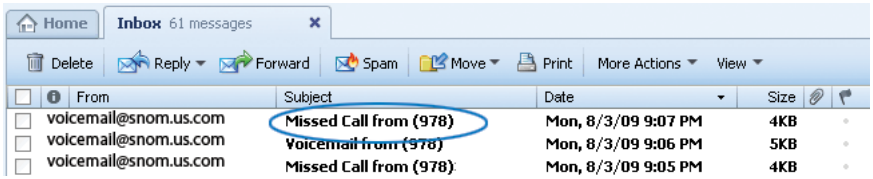


Note: Users can also use the *95/*96 star code from the phone to request that voicemail be sent as email attachments.

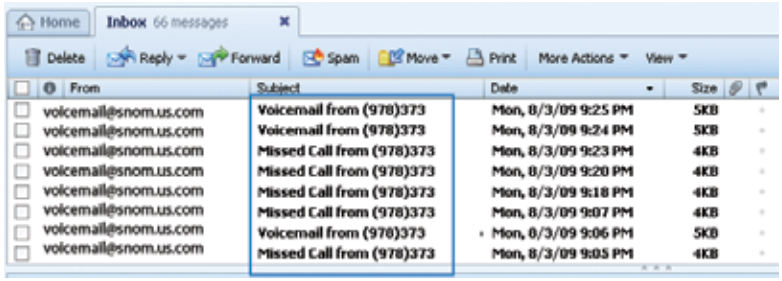
☎ * 9 5 Send voicemail as email (activate)

☎ * 9 6 Send voicemail as email (deactivate)

- **After sending a message**: The user must decide what to do with a voicemail message after it has been emailed:
  - **Keep message as new message**: The message will remain in the user mailbox as a new message. This option has the potential danger of eventually overfilling the user's voice mailbox.
  - **Mark message as read**: The message will remain in the user's mailbox, but the system will drop the oldest message to make room for a new message if the mailbox becomes full. The disadvantage of this mode is that the message waiting indicator will not alert the user of new messages.
  - **Delete the message**: The message will be deleted after the email has been sent. This keeps the user's mailbox clean, but the system does not store voicemail messages permanently. The user will have to listen to the messages from the email client.
- **Send email on missed calls**: When this setting has been activated, the system sends the user an email for each missed call (see below). Calls to a hunt group or agent group are not included.



- **Send email at the end of every call**: When this setting is activated, the system sends the user an email for all calls (see below). This feature is useful for keeping track of a group sales extension, a telemarketing campaign, or calls made to a new employee's extension. (When both "missed calls" and "all calls" have been activated, the user will receive two emails for each missed call.)



Note: Users can also use the Request Call Details (*63) star code to request the call details of a particular call. Details include the caller-ID, the duration of the call, and the time the call was made. This feature is handy and prevents users from having to ask the caller for contact information. Users must:

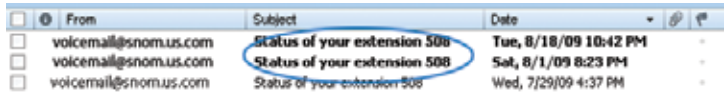
1. Dial *63 and press the confirm button on the telephone keypad.

2. Retrieve the message in their email account.

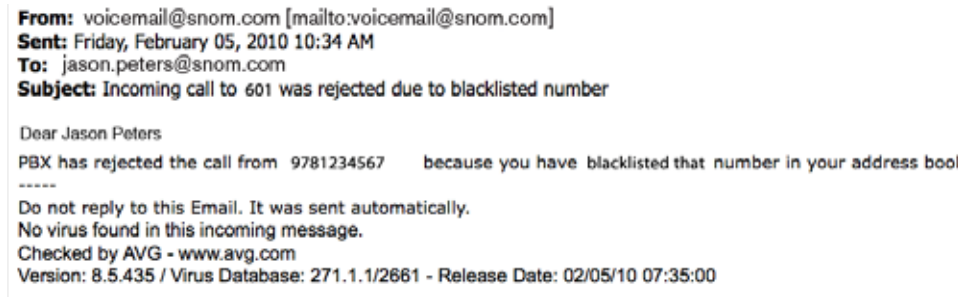
   Note: The email sent by the system includes a link to the last number. When users click the link, the system will prompt them for a username and password (in the form `user@domain`). If the user's browser supports saving the login information, the next time the user clicks such a link to dial a number, the call will immediately be initiated.

   This feature works only with user agents that support the REFER mechanism outside of existing dialogs. On some phones, users must press "Ok" or lift the handset in order to acknowledge the dialing of the number. The remote initiation of a call is a security-sensitive topic, as it might turn a user's phone into a microphone. Therefore, user's must authenticate themselves during the initiation of the call and may have to acknowledge the initiation of the call.

- **Send email on status changes**: The user will be notified of all status changes (e.g., changes to the DND status, the registration status, etc.).



- **Send email when mailbox is full**: The user will be notified when their mailbox is full.
- **Send email if call was rejected because of blacklisted number**: When users execute the *92 star code (Add to Blacklist) to block a particular caller (or if the caller is already tagged as a blacklisted caller in the user's address book), an email will be sent to the user's mailbox when that caller has attempted to call.


From: voicemail@snom.com [mailto:voicemail@snom.com]
Sent: Friday, February 05, 2010 10:34 AM
To: jason.peters@snom.com
Subject: Incoming call to 601 was rejected due to blacklisted number

Dear Jason Peters

PBX has rejected the call from 9781234567 because you have blacklisted that number in your address book

---

Do not reply to this Email. It was sent automatically.
No virus found in this incoming message.
Checked by AVG - www.avg.com
Version: 8.5.435 / Virus Database: 271.1.1/2661 - Release Date: 02/05/10 07:35:00

Receiving Email Notifications from the System

Types of Email Notifications

The system can be configured to notify a list of administrator accounts when an important system event occurs. The types of email notifications are presented in Figure 17-2 and are located in **Admin** > **Email** > **Messages**. To modify the text of these email notices or to improve the translation of the messages, refer to "Web Page Control" on page 74.

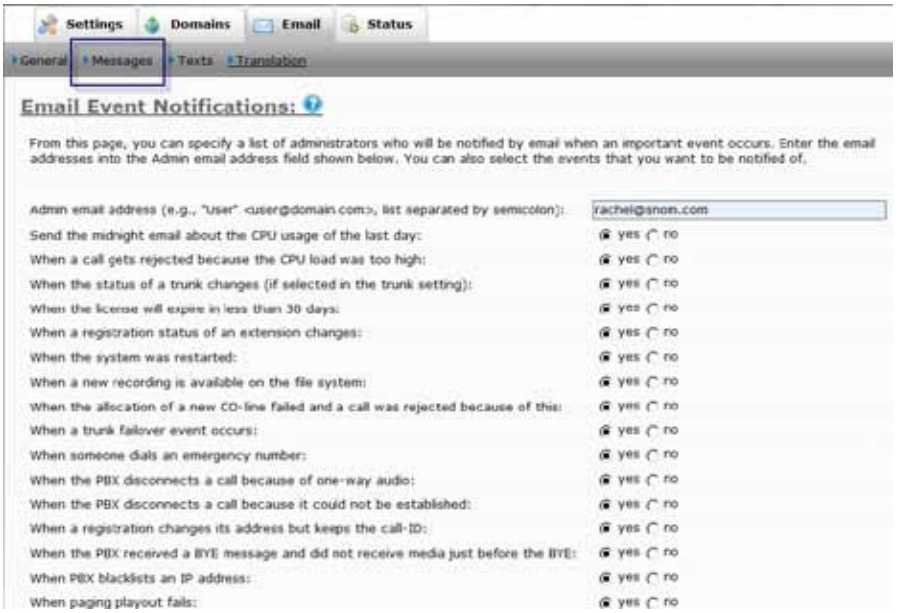

Settings
Domains
Email
Status
General
Messages
Texts
Translation
Email Event Notifications:
From this page, you can specify a list of administrators who will be notified by email when an important event occurs. Enter the email addresses into the Admin email address field shown below. You can also select the events that you want to be notified of.
Admin email address (e.g., "User" <user@domain.com>, list separated by semicolon):
rachel@snom.com
Send the midnight email about the CPU usage of the last day:
When a call gets rejected because the CPU load was too high:
When the status of a trunk changes (if selected in the trunk setting):
When the license will expire in less than 30 days:
When a registration status of an extension changes:
When the system was restarted:
When a new recording is available on the file system:
When the allocation of a new CO-line failed and a call was rejected because of this:
When a trunk failover event occurs:
When someone dials an emergency number:
When the PBX disconnects a call because of one-way audio:
When the PBX disconnects a call because it could not be established:
When a registration changes its address but keeps the call-ID:
When the PBX received a BYE message and did not receive media just before the BYE:
When PBX blacklists an IP address:
When paging playout fails:
yes
no

Figure 17-2. Types of Email Notifications

CDRs to Email

All types of CDRs can be exported to email. Depending upon which type of information you would like to receive, you will need to configure the respective setting on the snom ONE.

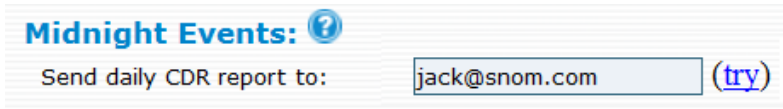
Important: Before you can receive any type of CDR, the **SMTP server** settings must be configured (go to **Admin** > **Email)**.

CDRs for Trunk Activity

If you want to receive a nightly email report on trunk activity, add your email address to the Midnight Events setting.

1. Navigate to **Domain**.
2. Click the domain.
3. Click **Settings**.

4. Scroll down to Midnight Events and enter your email address into the **Send daily CDR report** to setting.



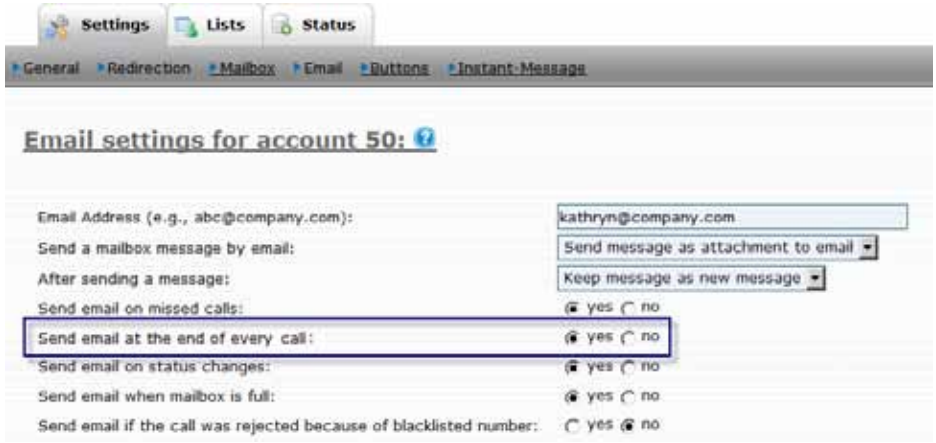
Note: When entering multiple email addresses into the field shown above, use semicolons between the addresses (e.g., `Fred Feuerstein <ff@domain.com>; Carl Clements <cc@domain.com>`).

Note: Clicking the **Try** button will send the CDR immediately. This allows you to see if your settings work, rather than waiting until midnight. Keep in mind that this is just a link, and you may have to save your list before clicking the link.

CDRs for Your Extension Only

If you want to receive emails for your calls only, add your email address to your extension and enable the **Send email record** setting:

1. Log on as a user.
2. Click **Settings** > **Email**.
3. Enter your email address into the **Email Address** field.
4. Click **Yes** for **Send email record for all calls**.

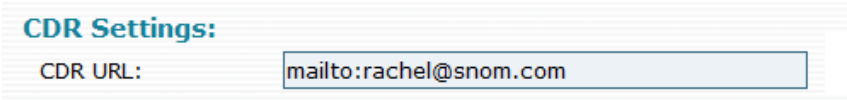


CDRs for All Extensions on Your Domain

If you want to receive emails for every call on every extension, add your email address to the **CDR URL** setting at the domain level.

1. Click **Domain**, then choose the domain.
2. Click **Settings**.
3. Scroll down to **CDR URL** and enter your email address.

   Note: You must use the `mailto` syntax as shown below.

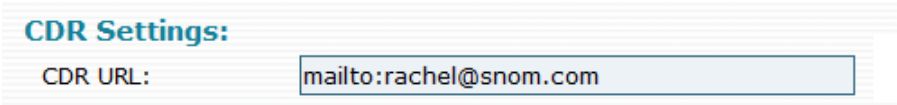


CDRs for All Extensions on All Domains

If you want to receive emails for every call on every extension for all domains, add your email address to the **CDR URL** setting on the **Admin** > **Settings** page.

1. Click **Admin** > **Settings**.
2. Scroll down to **CDR URL** and enter your email address.

   Note: You must use the `mailto` syntax as shown below.



The following report shows a running list of the previous day's calls:

From: voicemail@snom.com [mailto:voicemail@snom.com]
Sent: Thursday, October 29, 2009 12:00 AM
To: rachel@snom.com
Subject: Head Office: Calls on 2009/10/28

The following calls were made in the domain on 2009/10/28

Total number of calls: 154. Total duration: 9:22:26.

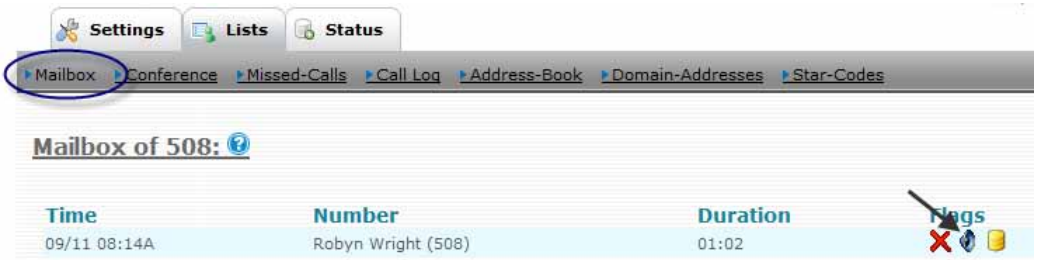
Time	From	To	Duration
2009/10/28 06:15:12	Jack Smith 9871234567	03031234567	00:02
2009/10/28 08:52:27	(604)1234567	(978)746-2777	00:03
2009/10/28 09:16:49	16621234567	19781234567	00:11
2009/10/28 09:16:25	1(662)862-8888	Stanley (506)	00:45

Figure 17-3. Sample CDR Report

Call Recording to Email

Two types of call recording are available on the system: system-initiated and user-initiated (also known as ad hoc). Only ad hoc recordings can be sent to email. With ad hoc recording, calls are recorded using either the **Record** button on the phone or by executing the *93/*94 star codes. See Chapter 18 for more information on call recording.

Depending upon which phone model is being used, the **Record** button may be located in different places on the phone. On the snom 360, the **Record** button has a white circle on it. When the button is pressed, the phone display will show a solid black circle to indicate that the call is being recorded. The recorded call will be displayed in the extension user's log under **List > Mailbox**. The user can click the audio icon to play the recording as shown below:

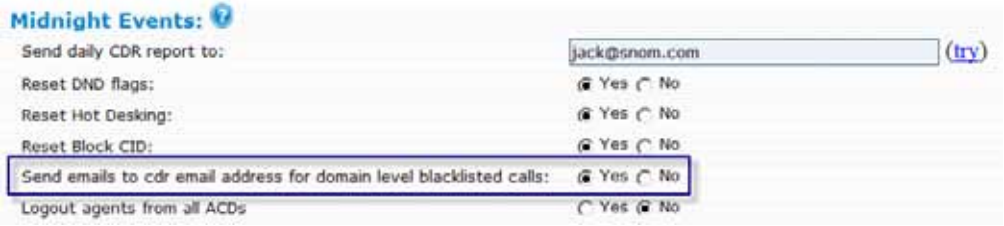


Blacklist Activity to Email

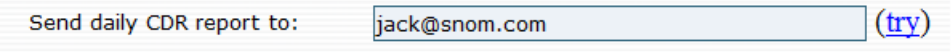
System-Initiated

To configure the system to send an email for domain-level blacklisted calls, configure the domain as follows:

1. Navigate to **Domains.**
2. Select the domain, then click **Settings**.
3. Scroll down to **Midnight Events**.
4. Enter an email address into the space provided.
5. Click **Yes** for the blacklisted option shown below:



The email will be sent at midnight to the specified CDR email address. For a trial run of the way this feature works, click **Try**.



An email will be sent to the email address you've indicated.

Chapter 18

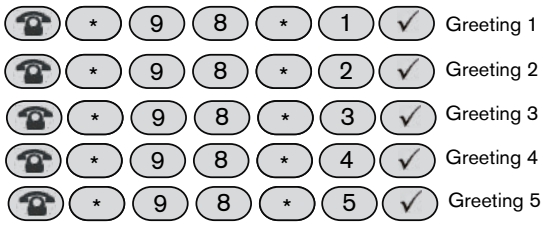
AUDIO AND GREETINGS

Greetings

Greetings are prerecorded, customized messages that can be used with numerous account types. Users can create greetings for their personal voicemail account, and administrators can create greetings for auto attendant, agent group, and IVR node accounts. Greetings are created with the Record New Greeting (*98) star code and are stored in the `recordings` folder. Users need permission before they can record greetings for domain accounts.

Personal Greetings

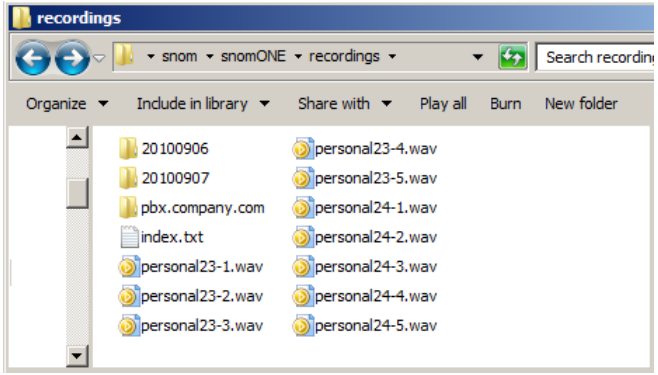
Users can record up to five greetings for their personal extension accounts. Greetings are created using the *98 star code followed by the greeting number:



Naming Conventions

Recorded greetings will appear in the `recordings` folder and are named according to the system's syntax rules. Its naming system is based on the greeting number that was recorded and the account type for which the greeting was recorded (personal, auto attendant, agent group, etc.). The actual account number is never reflected in the file

name of the greeting, as shown below (the numbers `23` and `24` are internal ID numbers assigned to two different extensions).



Activating a Personal Greeting

Administrators: Once greetings have been recorded for an extension, administrators have the option to upload them from the **Mailbox** tab of the user's account.

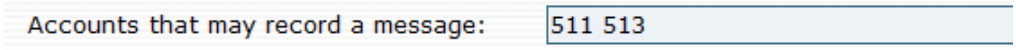
Users: Once greetings have been recorded, a user can activate a greeting by using the following steps:

1. Enter extension number to access voice mailbox.
2. Press 9 ("select mailbox greeting"), or press * to skip to the main menu.
3. Once you hear the greeting you would like to use, press the corresponding greeting number when the greeting has finished playing.

To delete personal greetings, navigate to the location where the greetings are stored on the system, and delete them.

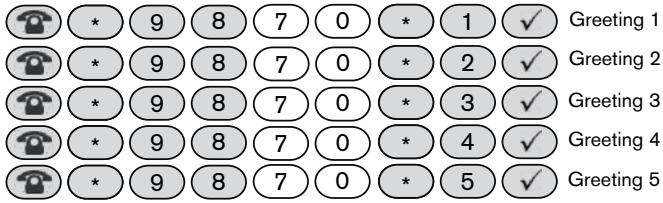
Auto Attendant Greetings

Users must have permission to record auto attendant greetings. This setting is located within the auto attendant account. The administrator must enter specific extension numbers into this field. An asterisk can be used to indicate that all users are allowed to record messages.



Auto attendant greetings can be created using the Recording New Greeting (*98) star code or by creating them yourself. Up to five greetings can be recorded.

Star code method: Any extension within the network that has permission to record auto attendant greetings can use this method for recording. The account number of the auto attendant must precede the greeting number. In the following example, `70` is the auto attendant. The greetings are automatically placed into the `recordings` directory.



Manual method: Only domain administrators can create greetings using the manual method, as access to the auto attendant account is required. This method requires that domain administrators create their own recordings and upload them through the **IVR** tab of the auto attendant account. Uploaded recordings should be 8 kHz mono, 16 bit files.

Naming Conventions

Auto attendant greetings (when created with *98) are named according to the system's syntax rules. Its naming system is based on the greeting number that was recorded and the account type (personal, auto attendant, agent group, etc.) for which the greeting was recorded. The actual account number is never reflected in the file name of the greeting, as shown below (the number `11` is an internal ID number).

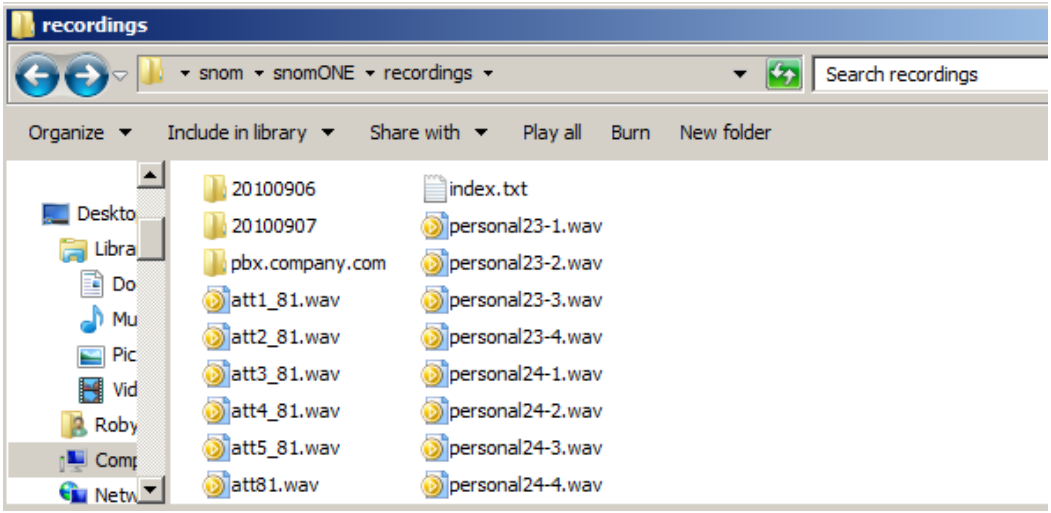
Table 18-1. Naming Convention for Auto Attendant Greetings

Account Type	Input	Internal Naming System	File Name
Auto Attendant	*9870*1	att1_<internal user ID>.wav	`att1_81.wav`
Auto Attendant	*9870*2	att2_<internal user ID>.wav	`att2_81.wav`
Auto Attendant	*9870*3	att3_<internal user ID>.wav	`att3_81.wav`
Auto Attendant	*9870*4	att4_<internal user ID>.wav	`att4_81.wav`
Auto Attendant	*9870*5	att5_<internal user ID>.wav	`att5_81.wav`

Note 1: Internal user IDs are generated by the system.

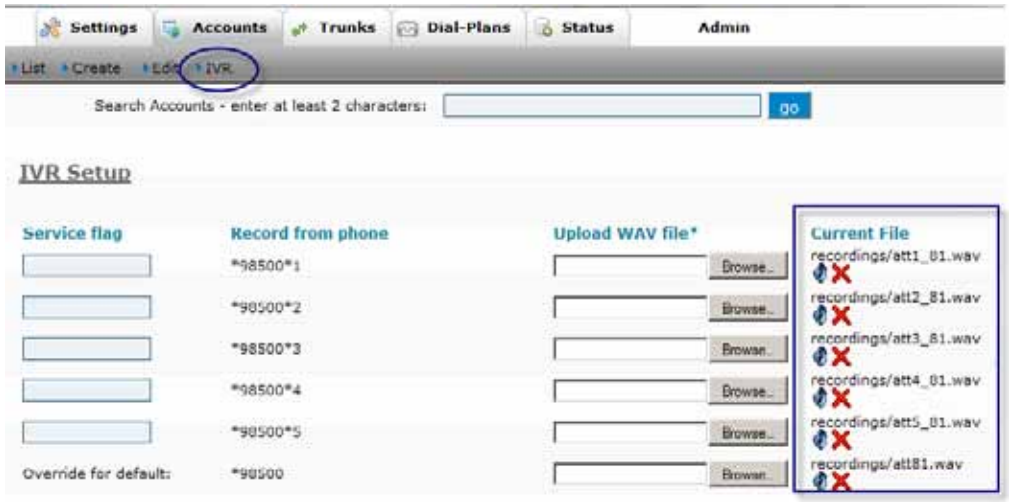
Note 2: "70" is the account number of the auto attendant.

The recordings will be stored in the `recordings` directory:



Activating Auto Attendant Greetings

Once auto attendant greetings have been recorded, administrators can activate them by creating **service flags** and uploading corresponding greetings.

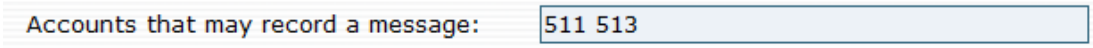


To delete auto attendant greetings, navigate to the location where the greetings are stored on the system, and delete them.

Agent Group Greetings

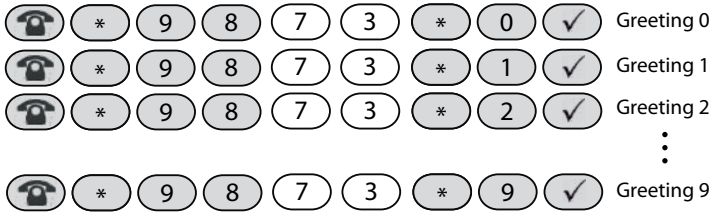
Agent group greetings can be used to provide callers with information about a company or to provide additional options for the caller (see "Mapping Telephone Keypad Numbers with Extensions" on page 240).

Users must have permission to record agent group greetings. This setting is located within the agent group account. The administrator must enter specific extension numbers into this field. An asterisk can be used to indicate that all users are allowed to record messages.



Agent group greetings are created using the Recording New Greeting (*98) star code and are automatically placed into the `recordings` directory. Agent group greetings can be recorded from any extension within the network that has permission to record

greetings. Ten greetings can be recorded (0 through 9). The account number of the agent group must precede the greeting number. In the example shown below, 73 is the number of the agent group. To listen to the greetings, dial the agent group number (e.g., 73).



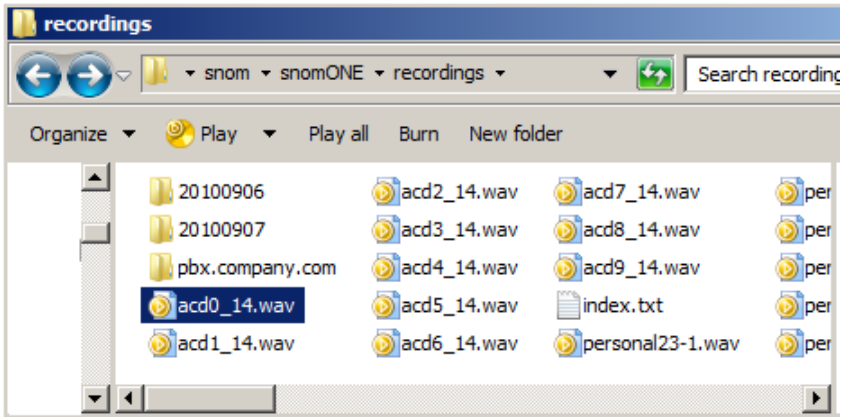
Naming Conventions

Agent group greetings (when created with *98) are named according to the system's syntax rules. Its naming system is based on the greeting number that was recorded and the account type (personal, auto attendant, agent group, etc.) for which the greeting was recorded. The actual account number is never reflected in the file name of the greeting (in the example shown below, the number 14 is an internal ID number).

Table 18-2. Automatic Naming Conventions for *98 Greetings

Account Type	Input	Internal Naming System	File Name
Agent Group	*9873*0	acd0_<internal user ID>.wav	acd0_14.wav
Agent Group	*9873*1	acd1_<internal user ID>.wav	acd1_14.wav
Agent Group	*9873*2	acd2_<internal user ID>.wav	acd2_14.wav
Agent Group	*9873*3	acd3_<internal user ID>.wav	acd3_14.wav
Agent Group	*9873*4	acd4_<internal user ID>.wav	acd4_14.wav
Agent Group	*9873*5	acd5_<internal user ID>.wav	acd5_14.wav
Agent Group	*9873*6	acd6_<internal user ID>.wav	acd6_14.wav
Agent Group	*9873*7	acd7_<internal user ID>.wav	acd7_14.wav
Agent Group	*9873*8	acd8_<internal user ID>.wav	acd8_14.wav
Agent Group	*9873*9	acd9_<internal user ID>.wav	acd9_14.wav

The recorded greetings are stored in the `recordings` directory:



Activating Agent Group Greetings

Once greetings have been recorded for the agent group, they will automatically play in sequence when a caller is waiting in the agent group queue. Once the messages have finished, they will restart. The gaps between the messages can be configured to span 5 to 180 seconds (gaps between announcements), during which music will be played. See Chapter 11 for more information on agent groups.

To delete agent group greetings, navigate to the location where the greetings are stored on the system, and delete them.

Recorded Phone Calls

One minute of call recording consumes approximately 100K of disk space. Using this estimate, Table 18-3 details the disk space requirements for a 10-person and 100-person call center. This does not take into account the compression feature, which could potentially increase that number by a factor of 8. (The CPU processor is compromised during compression and the quality of recordings is reduced, so turn on compression only if your disk space is limited and you have a good CPU.)

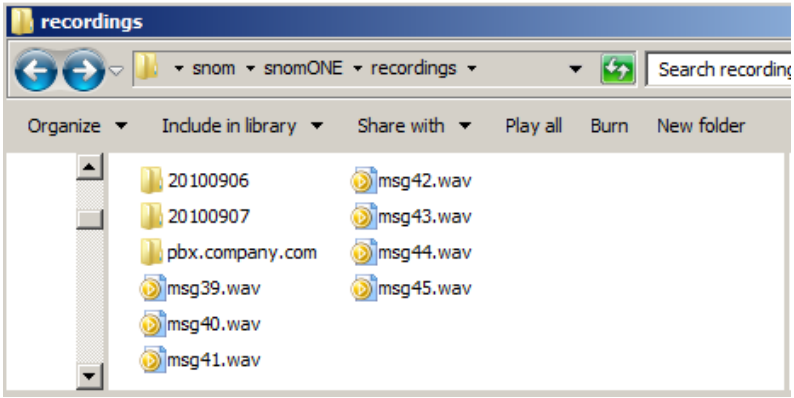
Table 18-3. Recordings and Disk Space Requirements

Recorded Time	Disk Space Requirements		
	Per Person (Mb)	10-Person Call Center (Mb)	100-Person Call Center (Gb)
15 minutes (0.25 hour)	1.5	15	1.5
30 minutes (0.5 hour)	3	30	3
60 minutes (1 hour)	6	60	6
120 minutes (2 hours)	12	120	12
240 minutes (4 hours)	24	240	24
480 minutes (8 hours)	48	480	48

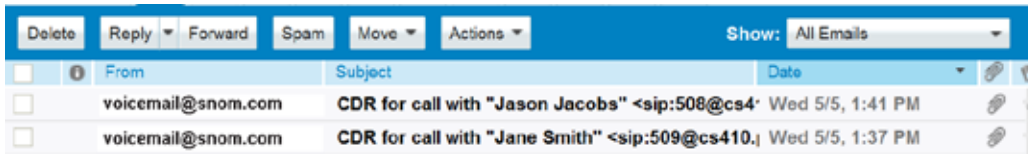
Two types of recordings can be produced on the system: user-initiated and system-initiated. These are discussed below.

User-Initiated Recordings

User-initiated recordings are generated when the user either presses the **Record** button on an IP phone (e.g., snom 320 and 360) or dials the Record (*93) star code. The recordings will be placed into the `recordings` folder. Anyone with access to the computer running snom ONE can listen to, copy, save, and forward the conversations.

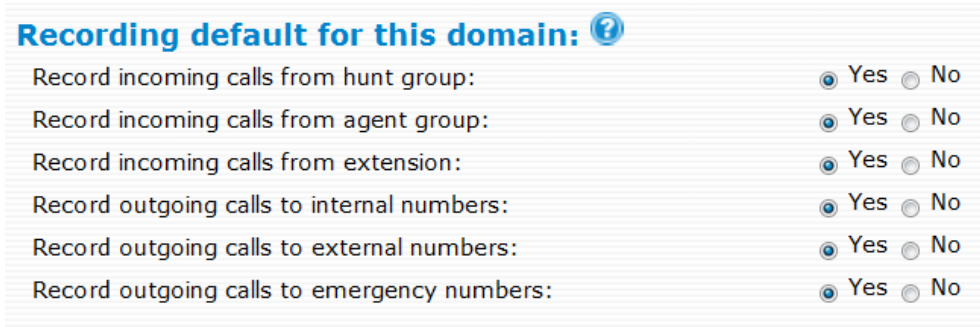


The recordings will be sent to the user's email address. Users can listen to them by clicking the paper clip.

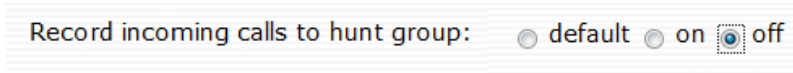


System-Initiated Recordings

System-initiated recordings include calls that are automatically recorded by the system. A domain can be configured to automatically record the following types of calls:


Recording default for this domain:
Record incoming calls from hunt group: Yes No
Record incoming calls from agent group: Yes No
Record incoming calls from extension: Yes No
Record outgoing calls to internal numbers: Yes No
Record outgoing calls to external numbers: Yes No
Record outgoing calls to emergency numbers: Yes No

This list can be accessed in **Domains** > **Settings** (see page 104). The settings that are made there will serve as the recording defaults for the indicated accounts across the domain. If you have multiple hunt groups and/or agent groups on the system and would like to override the default recording settings for some of those accounts, you can use the **Record incoming calls to hunt groups** and **Record incoming calls to agent groups** settings in the account itself.



File System

The file location and file name of system-initiated recordings are determined by the **Record Location** setting (page 47). The **Record Location** string is a two-part string.

The first portion of the string determines the location of the recording, and the second determines the name of the recording.

Storage Location	File Name
$r/$o/$a/	$d-$t-$i-$n.wav

Using the string shown above (which is the system default), the directory location would be `snomONE/recordings/pbx.company.com/73`, and the file name could be `20100907-165929-i-50.wav`.

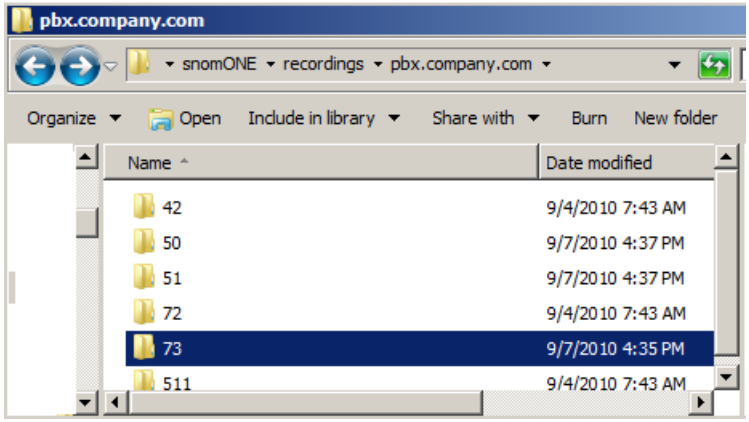
There's a lot of flexibility with regard to where the system can place recordings and the file names that it assigns. Following are the variables that can be used in the **Record Location** field:

Table 18-4. Syntax for Recording to File

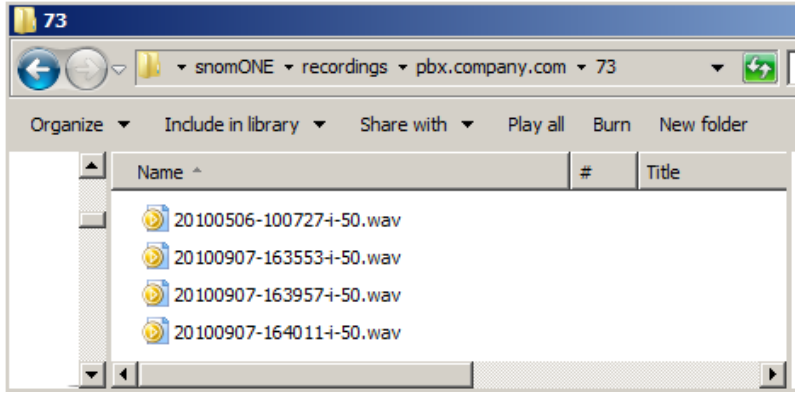
Syntax	Definition	Description
`$r`	Recordings	The location (e.g., the `recordings` directory)
`$o or $m`	Domain	A subdirectory (`recordings/CompanyA`)
`$a`	Account	The number of the account (e.g., 40, 70, 73)
`$d`	Date	The date of the call (e.g., `20071220`)
`$t`	Time	The time of the call, e.g., `134349`
`$i`	Direction of call	The system substitutes an `i` for incoming calls, and an `o` for outgoing calls.
`$n`	Number	The calling party's number. Depending on the direction of the call, this field could reflect the number of either the calling or called party.
`$u`	Extension	The primary name of the extension. Depending on the direction of the call, this field could reflect the number of either the calling or called party.
`$x`	Connected agent in ACD/hunt group calls	Connected agent in ACD/hunt group calls
`$l`	Caller-ID	

Syntax	Definition	Description
`$c`	CMC	Client matter code
`$$`		Produces a single $ symbol

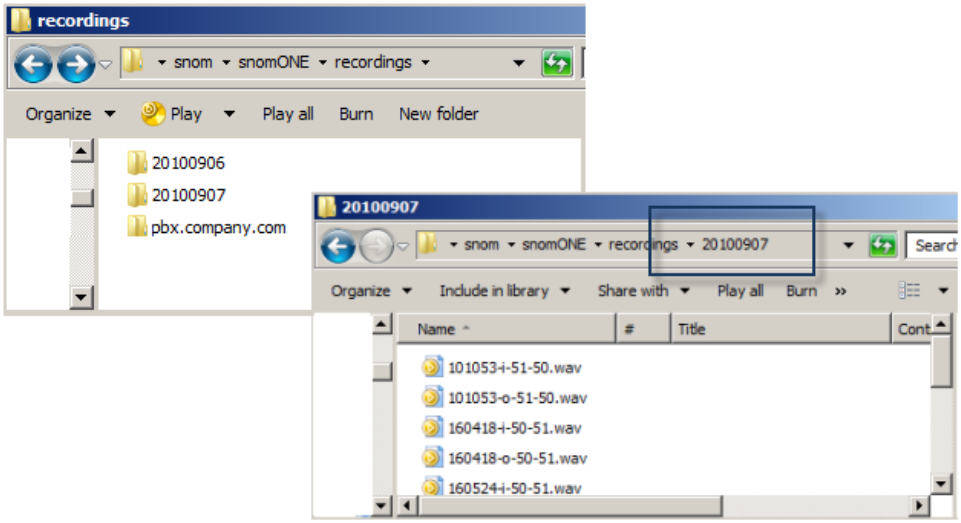
As mentioned earlier, the default setting is `$r/$o/$a/$d-$t-$i-$n.wav`. The recording will be placed into the `recordings/<domain>/<account>` directory as shown below:



The files inside the directory will reflect the date and time, direction of the call, and the calling party:



Recordings can also be categorized according to date. The following recordings were generated on September 7, 2010, using the string `$r/$d/$t-$i-$u-$n.wav`.



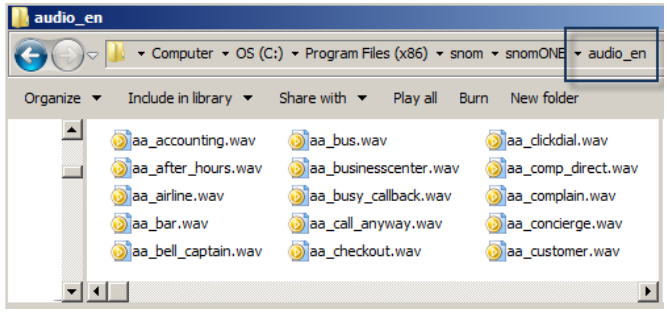
Notes

The `recordings` directory is relative to the working directory of the system and contains other WAV files, such as mailbox messages and greetings. If you would like to create a new directory for recordings, you must first create the directory before using it. The directory path must always be relative to the working directory of the system.

When `$u` and `$n` are used at the domain level (e.g., `$r/$d/$t-$i-$u-$n.wav`), the recorded files will be created under `<pbx-install-dir>/recordings/<date>` directory, and the file will reflect the time the call was made, the direction of the call, and the extension number of both the calling party and the extension that was called. However, the filename will be based on whether the call was incoming or outgoing. For example, if extension 601 calls extension 604 (and **Record incoming calls from extension** has been set to **Yes**, as shown below), the resulting file will be `095404-i-604-601.wav` (`$i` is the direction). Note that `$u` output represents the called party and `$n` the calling party). And if extension 601 calls extension 604 (and **Record outgoing calls to internal numbers** has been set to **Yes**), the resulting file will be `102019-o-601-604.wav`. In this case, the `$u` output represents the calling party and `$n` the called party.

Audio Prompts

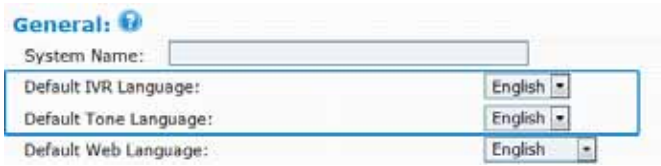
The voicemail and IVR systems of the snom ONE rely on audio prompts for their menu prompts. By default, these prompts are in U.S.-English and are located in the `audio_*` directory.



The prompts are easily identifiable by their 2- and 4-digit prefixes.

Prefix	Description
`aa-`	Auto attendant
`bi-`	Built-in numbers
`co-`	Conference
`code-`	Feature code related
`ex-`	Extension-related
`mb-`	Mailbox
`pb-`	ACD (agent group)
`wk-`	Time-related

Some administrators will need to download additional languages so that non-English-speaking users can hear prompts in their own language. When additional languages have been uploaded into the system, those languages will be available in the **Default IVR Language** and **Default Tone Language** dropdown lists:



Uploading New Languages

Audio prompts in many languages can be downloaded from snom ONE's web site. Following is a list of available languages:

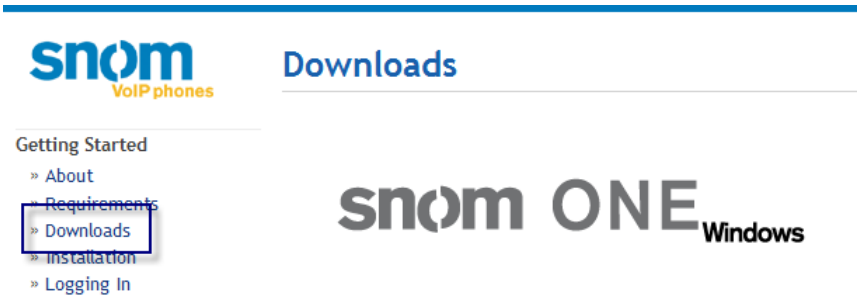
Table 18-5. Country Identifier Codes

Country	Identifier
Brazilian	br
Danish	dk
Dutch	nl
English	en
English	uk
French (France)	fr
French (Canada)	ca
German	de

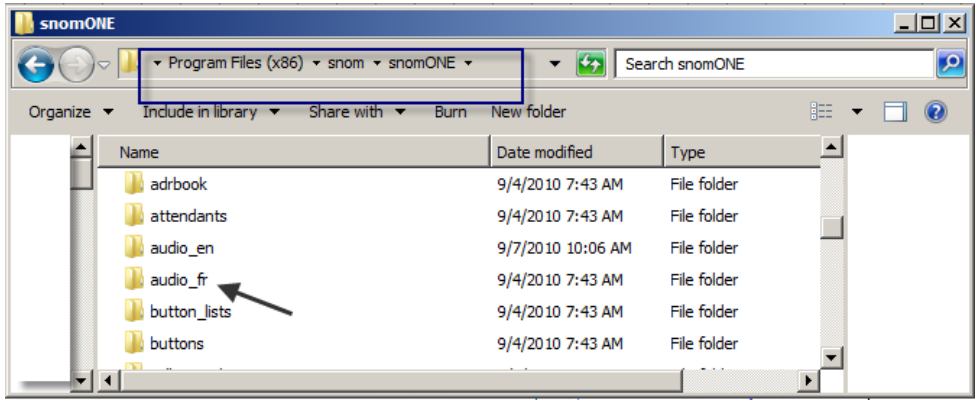
Country	Identifier
Greek	gr
Italian	it
Polish	pl
Russian	ru
Spanish	sp
Swedish	se
Turkish	tr

To download a set of audio prompts:

1. Go to wiki.snomone.com and click the **Downloads** link at the left:

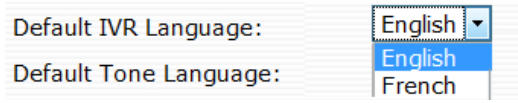


2. Place the new language into the `snom/snomONE` directory. The new language will be displayed next to the default language:



3. Restart the system.

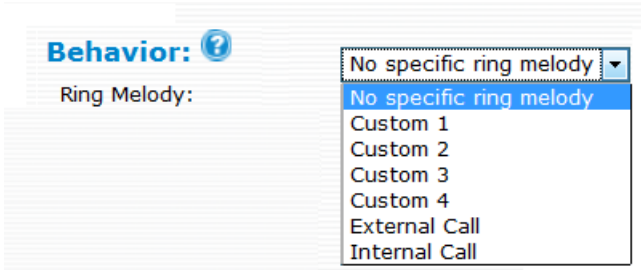
   The new language will be displayed in the language dropdown lists:



   Note: The **Default Tone Language** setting controls the ringback and busy tones that a caller hears during voicemail prompts and IVR interaction.

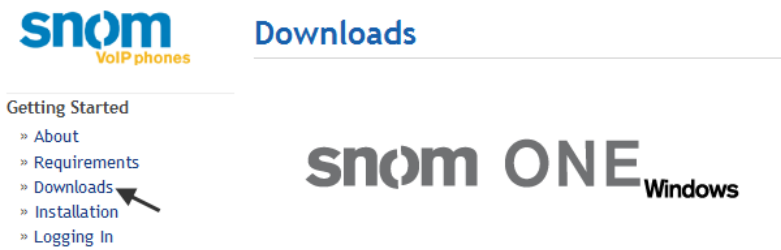
Customized Ringtones

Agent groups and hunt groups can be configured with distinct ringtones so that users answering calls on these groups will be able to determine which type of call is coming in. Once custom ringtones have been configured, they can be selected from the **Ring Melody** dropdown in the hunt group and agent group account.



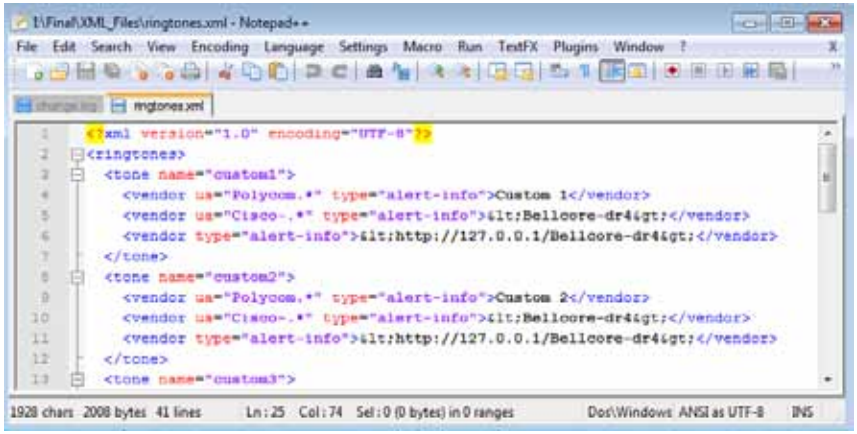
To create custom ringtones, you will need to come up with your own ringtones and link them to the snom ONE by modifying the `ringtones.xml` file. The following instructions show you how to configure custom ringtones for a snom phone:

1. Go to wiki.snomone.com and click the **Downloads** link at the left.



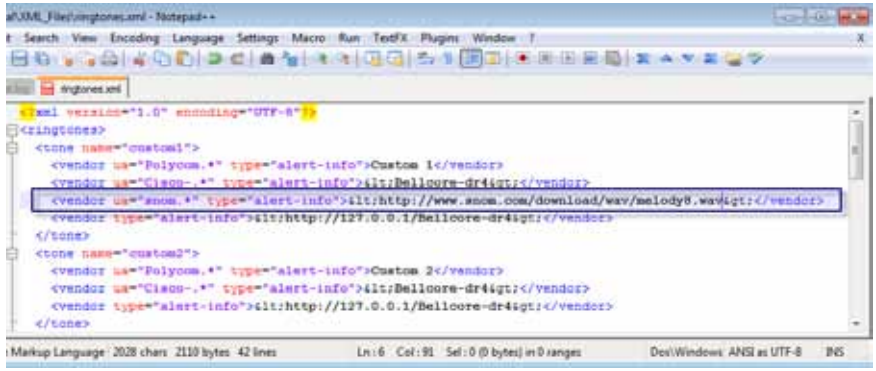
2. Scroll toward the bottom and click **Custom Ringtone Configuration File**.
3. Download the file, then open it in a text editor (e.g., NotePad++). The image shows a number of `vendor` elements that address various phone models (Polycom, Cisco). Phone models not indicated will automatically use the ringtone that is linked to the following address:

```
<vendor type="alert-info">&lt;http://127.0.0.1/Bellcore-dr4&gt;</vendor>
```

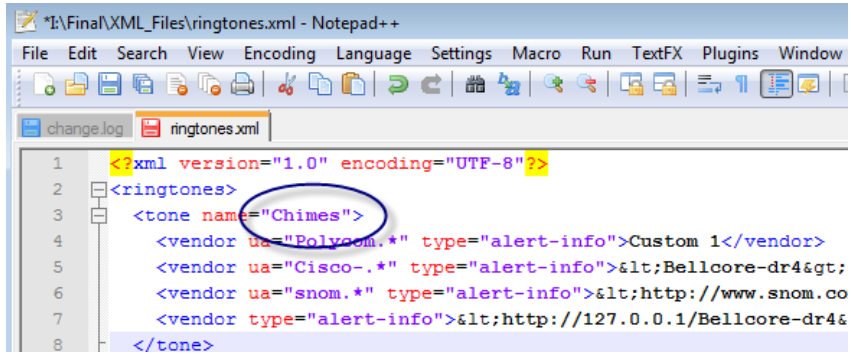


4. To create a custom ringtone for the snom ONE, create a new `vendor` element using one of the other vendor elements (copy and paste it).
   - For the `ua` atttribute, enter `snom.*`
   - Enter the URL of the wav file.

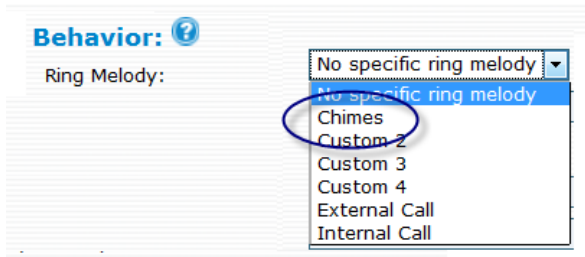
```
&lt;http://www.snom.com/download/wav/melody8.wav&gt
```



5. Replace `custom1` with a tone name that reflects the actual tone, in this case `Chimes`.



6. Save the file.
7. Place the file into the `html` directory (you may need to create the directory).
8. Restart the system.
9. The new tone will be listed in the **Ring Melody** dropdown:



Chapter 19

BUTTONS

Buttons simplify the workflow in almost any environment and are ideal for all types of users. Once a button has been configured to the user's extension, the user can press the button to execute whatever function has been configured to it. Button functionality includes many helpful options, including agent log in/log out and queue monitoring. These features allow call centers to provide an easy method to agents logging in and out of agent groups all day and for queue managers monitoring the queue. Button functionality simplifies almost any dialing sequence. Figure 19-1 shows the available options (each button type is detailed in Table 19-1 on the following page).

Buttons are part of a plug and play profile that has been configured to the user's extension and provisioned to the phone.

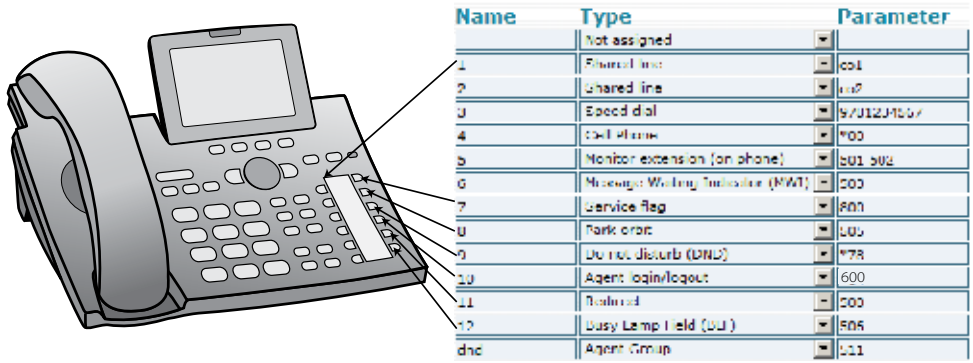


Figure 19-1. Button Functions

Table 19-1 describes each type of button that can be configured on the phone. When defining the buttons, you can use phone numbers, extensions, star codes, as well as other numbers, such as the direct dial prefix.

Table 19-1. Button Types and Parameters

Button Type	Parameter
Private: Multiple lines can be configured on IP phones. Indicate those extensions here.	`508 502`
Shared Line: Shared lines can best be compared to physical lines between the system and the central office. In the past, PBX users seized a line before they placed outbound calls. The shared line mode emulates this mode. When a user seizes a shared line, other users also sharing this line see the LED go on. Users can place calls on hold by pressing the button, and other users sharing this line can pick the call up by pressing the button again. This is sometimes referred to as "key system" functionality.	The name of a CO line in the domain (e.g., co1).
Speed Dial: When buttons are used as speed dials, the phone will simply dial the programmed number (the LED next to the button will not light). Speed dials can be used for phone numbers, extensions, star codes, and other numbers. For example, if you want to transfer a ringing call to the voicemail of a specific extension, the parameter would need to include the following: ■ The "transfer" star code (`*77`) ■ The **direct dial prefix** (e.g., `8`) ■ The number of the extension (e.g., `40`) Example: `*77840`.	`9781234567` `501` (call an extension) `*92` (blacklist a caller) `*00501` (speed dial 501's cell phone) `*77840` (transfer a call directly to 40's voicemail)
Cell Phone: This mode allows you to quickly call someone's cell phone. (After pressing the button, you will need to enter that person's extension number.)	`*00`

Button Type	Parameter
Monitor extension (on phone): Use this mode if you want to see the call status of another extension. (For snom phones, use the "on the phone" mode.) The extended mode is intended for the WAC. The monitoring is not passive: When a call is either coming in on that extension (fast blinking) or is on hold or parked (indicated by slow blinking), you can pick the call up by pressing the button. Calls that are connected have a solid color.	`501 502`
Service Flag: This mode allows you to change the status of a service flag. (This button type only affects service flags that can be changed manually; it will have no impact on automatic, time-dependant service flags.) See "Service Flags and Buttons" on page 191 for instructions.	`800` (an example of a service flag account)
Park Orbit: Use this mode if you want to assign a button to a park orbit (see Chapter 7 for instructions on creating a park orbit account). This button can be used in a number of ways: ▪ If no parameter is indicated, the call will be parked on the user's extension. ▪ If a park orbit is indicated, the call will be parked on the park orbit specified. Once this button has been configured, calls can be parked and retrieved by pressing this button. A parked call is indicated by a blinking light. Important: Before you can use this button, the star codes for Call Park and Call Park Retrieve must match (e.g., *85/*85).	Enter nothing (this parks the call on the user's extension) 505 (this parks the call on the extension number that is being used as a park orbit)
Do not disturb: This mode shows that extension's DND status. The LED will light when DND is in active mode.	`*78`

Button Type	Parameter
Agent login/logout: This mode shows an agent's login/logout status. This button can be used in a number of ways: ▪ If the agent needs to log in and out of all agent groups at the same time (or if the agent belongs to only one agent group), use a single **Agent login/logout** button and do not specify a parameter (leave it blank). ▪ If the agent belongs to numerous agent groups and needs to log in and out of a specific agent group before logging into another agent group, use multiple **Agent login/logout** buttons and in the parameter field, enter the agent group number. Do this for each agent group. Once this button has been configured, the LED will light when the agent is logged in. **Important**: Before you can use this button, the star codes for Agent Log in/Agent Log out must match (e.g., *64/*64).	If you enter nothing, it will log the agent out of all agent groups. If you enter a specific agent group (e.g., `511`), it will log the agent out of that agent group.
Redirect: This mode allows you to redirect calls to a predefined extension or number. To use this mode, enter the redirection target into the parameter field. Pressing the button activates redirection and lights the LED. Pressing the button deactivates redirection. This mode is useful when an executive assistant should take over calls.	`503` (quickly redirect a caller to 503)
Busy Lamp Field (BLF): This mode shows when the specified extensions are in use. When the extension is connected, the LED will be solid; when the extension is ringing, the light will blink fast; and when the extension is holding a call, the light will blink slowly. This mode is similar to the monitor extension mode; however, it does not support the picking up of calls. When the user presses the button, the phone always dials the programmed extension.	Extension number(s) to be monitored

Button Type	Parameter
Agent Group: This button allows users to monitor the status of an agent group. When a caller is waiting in the group, the LED will blink quickly. Users can then press the button to pick up the call.	`511` (account number of agent group)
Message Waiting Indicator (MWI): This button indicates when a message has arrived for the account that is entered into this field. The MWI button can be especially useful in situations where it is necessary to send the same voicemail to more than one extension. In this case, a group mailbox must be created, and the phones must subscribe to MWI for the extension of the groupmail account. (This button can also be used for older phones that do not have a Message button on the telephone keypad.)	Extension number of a group sales account, for example.

Creating a Button Profile

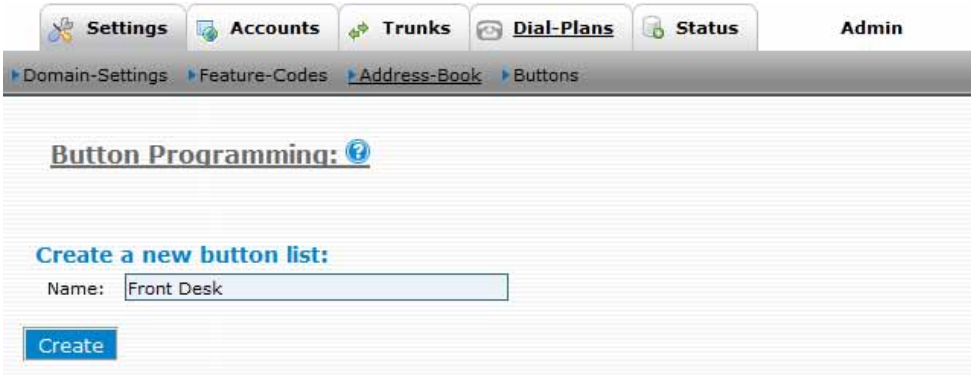
Before the buttons feature can be used, a button profile must be created. Users can create their own profile, or domain administrators can create profiles so that users across the domain can select from a list of profiles that have been pre-configured.

Two methods are available for creating profiles: the point-and-select method (which provides a dropdown from which you can choose the button type and add values) and the CSV approach (which allows you to enter each record directly into the web interface).

Point-and-Click Method

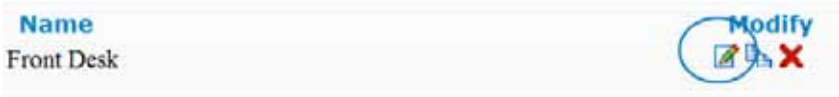
1. Navigate to **Domains** > **Settings**, and click **Buttons**.

2. Enter a name into the **Create a new button list** field.



3. Click **Create**. The new profile will be listed under **Name** as shown below:

4. Click the edit icon (the pencil).



5. To create a new button, enter a name for the button. Allowable values include `1` through `38` and `dnd`. Numerically, the values cannot exceed the number of buttons that are available on the phone. If you have a 12-button phone, the values must range from `1` to `12`. If `dnd` is used for one of the buttons (for a phone that does not have a DND button), replace the numerical reference with `dnd`.

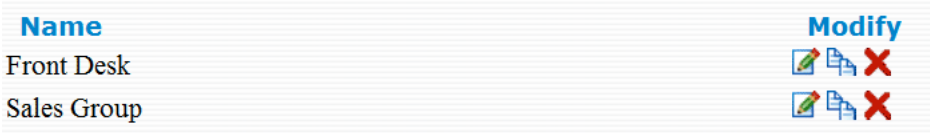
The values assigned to the buttons correspond with the positioning shown below:

Figure 19-1. Values to use for Button Profiles

6. From the dropdown, select the type of button you want to use (see Table 19-1 for a description of each button type).

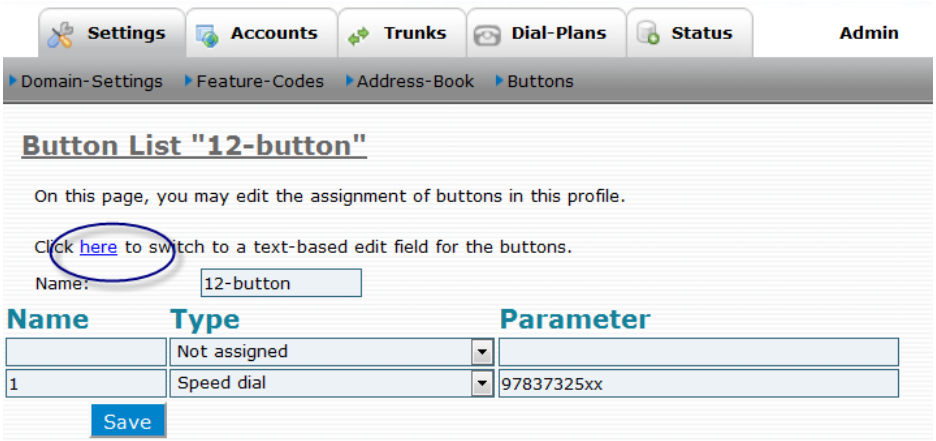
7. Enter a parameter (see Table 19-1).
8. Click **Save**.
9. Repeat Steps 5 through 8 for each additional button.

10. To create additional profiles, repeat Steps 2 through 9. New profiles will be listed under **Name** as shown below:



CSV Method

1. Complete Steps 1 through 8 from the "Point-and-Click" method (previous pages). The result will be one button profile with only one button set.

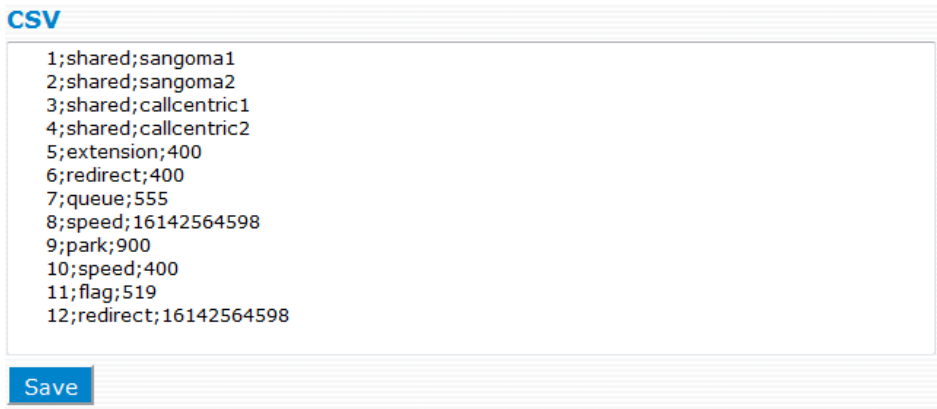


2. Click the **here** link as shown above to switch to a text-based editing window. A text-based editing window with one button record will be displayed:

3. Follow the same format for the other buttons, using the following table for the button types and Table 19-1 for the parameters.

Button Type	CSV Syntax
Private line	`private`
Shared line	`shared`
Speed dial	`speed`
Cell phone	`cell`
Monitor extension (on phone)	`extension`
Monitor extension (on PAC)	`long`
Service flag	`flag`
Park orbit	`park`
Do not disturb	`dnd`
Agent login/logout	`login`
Redirect	`redirect`
Busy lamp field (BLF)	`blf`
Agent group	`queue`

4. When finished, click **Save**.

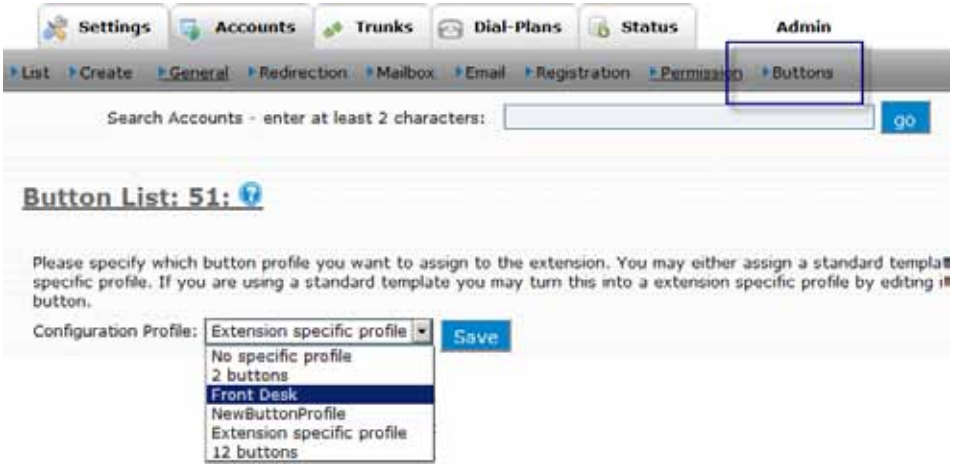


Assigning Button Profiles to Users

A button profile can be assigned to a single user or to multiple users. The following procedures outline both scenarios.

Assigning a Profile to a Single User

1. Navigate to **Domains** > **Accounts**.
2. Open the extension account.
3. Click **Buttons**.



4. From the **Configuration Profile** dropdown, select the profile you want to use.
5. Click **Save**.

   The new profile will be sent to the phone. Rebooting should not be necessary. On rare occasions, it may be necessary to reset the phone to force the phone to take on the new button mapping.

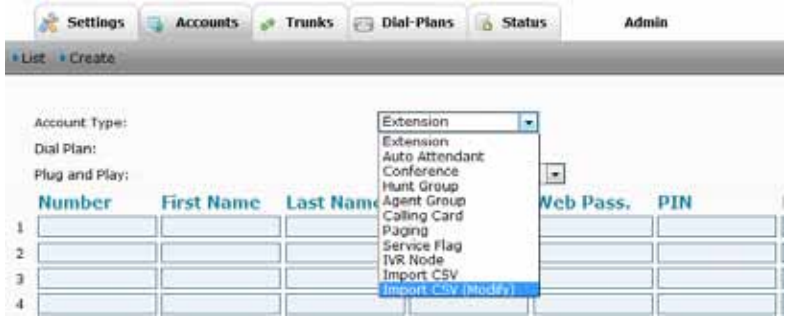
Massive Update of Profiles

Using the single-user method shown above, you can assign the same button profile to multiple users, but if a large number of extensions are involved, the process would be unnecessarily time consuming. A quicker approach would be to use a CSV file at the time you create the account/extension (see Appendix A for instructions on creating ac-

counts with CSV). If you have already created the extensions, you can still use the CSV approach. In this case, you will need to modify the extension information by importing a CSV file that reflects the button profile information. Following are instructions:

1. Create your CSV file using the instructions shown in Appendix A. Keep the following in mind:
   - The values you assign to `type` and `alias` must match the extensions' existing values for these parameters.
   - The parameter that is used for the button profile is `profile`. Be sure to assign the correct value to this parameter (the value is the name of the button profile). Using the list of profiles shown below, the values would be `12 buttons`, `2 buttons`, and `Front Desk`.

2. Navigate to the **Accounts** tab.
3. Click **Create** (top left).
4. From the **Account Type** dropdown, select **Import CSV (Modify)**.



5. Click **Create**.

Key System Configuration

The buttons feature can be used to emulate a key system when combined with a snom phone. Although there are no physical cables to connect the snom ONE telephone system with the outside world, as with a TDM-based PBX, it is still possible to emulate the behavior of TDM-based PBXs and still have "CO-lines."

CO-lines are associated with trunks, and each trunk may have several. CO-lines are listed in the account list because they share the same namespace.

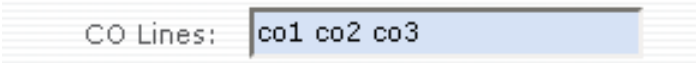
Once configured, the buttons will have the following behavior:

- When a corresponding extension receives a call, the button will blink (by pressing the button, the call can be picked up).
- When the corresponding extension is busy, the button will light.
- When the button is pressed while the extension is idle, the button will call the extension.

Setting up a Key System

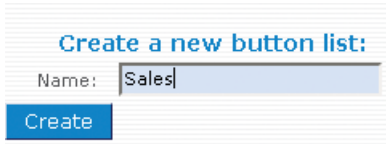
Important: Before beginning this procedure, do plug and play for the phone that is being configured (see Chapter 20).

1. Set CO lines on trunk (this setting is made on the trunk). Enter the name of each CO-line.

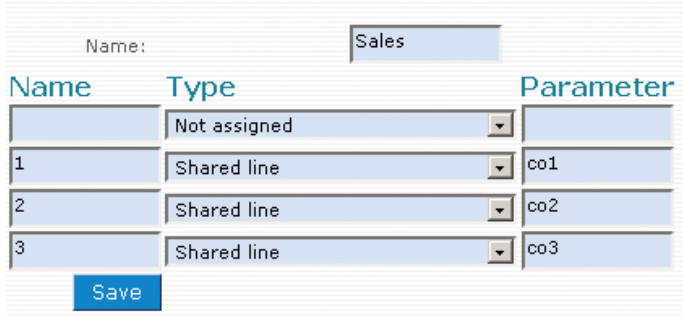


Note: Because users can subscribe to the state of the CO-lines, the names given to CO-lines must be unique across the domain. For example, you can set up four CO-lines on Trunk1 with the names "co1 co2 co3 co4" and more CO-lines on Trunk2 with different names like "co5 co6 co7 co8" (the list of CO-lines must be separated by a space). The system will reject names for CO-lines that are already used by accounts or other CO-lines in the same domain.

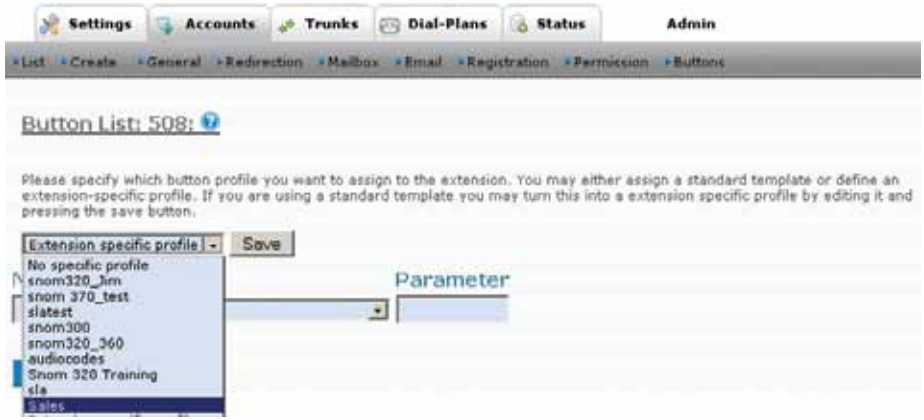
2. Create a buttons profile for the phone. Do this by going into **Domains** > **Buttons**. Enter a name for the buttons lists (the name must be unique across the domain). Then click **Create**.



3. In the buttons profile you just created, create a button for each of the co-lines from Step 1. To do this, name the button (e.g., `1`), choose **Shared line** from the dropdown, then enter the name of the co-line (e.g., `co1`). Click **Save**. Repeat this step for each button.



4. From the user's extension account, click **Buttons**. From the dropdown, choose the buttons profile you just created, and click **Save** to assign it to the extension.



To verify that the phone received the plug and play configuration, you will need to check the function key configuration from the snom GUI. This is detailed in the following steps:

1. Enter the IP address of the phone into a web browser (e.g., `http://192.168.1.3`). If you don't know the IP address, press the question mark key on the phone. The IP address will show in the telephone display.
2. Click **Function Keys** at the left of the screen.

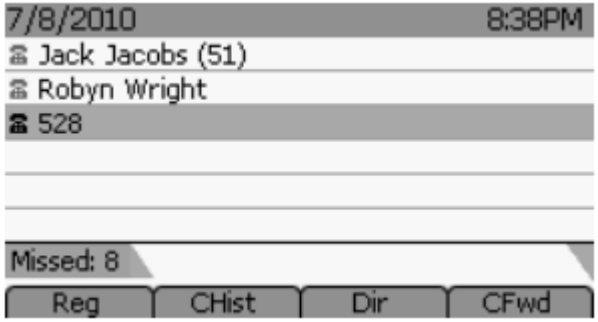
   Toward the lower half of the screen, the buttons that have been configured for **Button** will be listed.

Notes

- Key systems operate on the lines and not on extensions. If a call comes in on line 1, then everyone will see line 1 flashing. When the call is answered, the light will go solid on everyone's phones. If the call is put on hold, everyone's light will flash again.
- This method is simple compared to parking and picking up a call on the extension.
- Key system emulation is good for small offices but is not practical for large enterprises, as there would be too many lines to monitor on a T1.

Multiple Identities and Button Profiles

Multiple identities on a single phone (shown below) can be problematic with button profiles because a phone can utilize only one button profile at a time. When multiple identities are involved, the tendency is to configure a button profile that includes a private line for each user, which is okay to do. The problem occurs when a new button profile gets uploaded after the first one and overrides the private line settings. In these cases, it may be wiser to manually configure a button profile on the handset instead of using plug and play.



Chapter 20

PLUG AND PLAY

The goal of plug and play is for the phone to be able to find the snom ONE and download its configuration settings with little or no configuration. In many cases, this can be done without actually touching the phone. Plug and play gives the phone accessibility to many system settings and features that can be configured by the system, making it unnecessary to configure these settings on the phone itself. When plug and play is done properly, setting up a group of IP phones is as easy as setting up a series of analog phones, removing the need to manually configure each and every phone.

Finding the snom ONE

So how does the phone find the snom ONE? In most environments, the phone will find its IP settings automatically via a DHCP server. Once a DHCP is found, it will learn its IP address, subnet mask, default gateway, and DNS server. Once the phone can access the network, it can start looking for the snom ONE and begin provisioning its configuration files. How the phone actually finds the snom ONE is governed by whether the snom ONE is local or remote. Table 19-1 shows the possible scenarios and the protocols that are used to facilitate each.

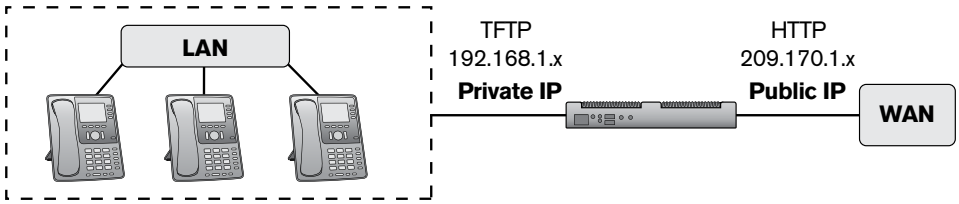
Table 20-1. Plug and Play Methods

Method	IP Address Locator	LAN	WAN	Touch-Free		Requirements
				Yes	No	
DHCP, option 66	DHCP	✓		✓		DHCP server must support opt. 66.
SIP SUBSCRIBE (multicast)	Multicast	✓		✓		Limited to a single snom ONE.

Method	IP Address Locator	LAN	WAN	Touch-Free		Requirements
				Yes	No	
Mass deployment	HTTP, TFTP, or HTTPS	✓	✓	✓		snom must have your server info and MAC address.
Manual setup	HTTP	✓	✓		✓	All settings must be configured manually.

Each plug and play method shown in Table 19-1 is described below:

- **DHCP, option 66**: This method can be used to provision in both LAN (internal) and WAN (remote) environments as long as you can control the local DHCP server and the DHCP server supports option 66. Once the extension has been created, all configuration settings are made using the GUI of the phone. The phone retrieves its IP address and other configuration information through dynamic host configuration protocol (DHCP). While this method can be used to find the snom ONE on the WAN, it cannot guarantee that the phone's MAC address will not be spoofed. Because of this, the user will be prompted to enter the password on the phone. (On the LAN, the snom ONE looks in its ARP cache and is 100% sure who it is talking to, so users on the LAN will not be required to authenticate.) Instructions using this method begin on page 352.



- **SIP SUBSCRIBE (multicast)**: Multicast plug and play is generally used when the DHCP server does not support option 66. Since multicast packets cannot be routed over the public Internet, this method cannot be used if the phone is connected remotely. With this method, the phone gets its IP address from the DHCP server and multicasts the SUBSCRIBE message with its MAC address, vendor information, model information, and the version

number. This method requires no configuration on the phone, but the **Listen to sip.mcast.net** setting will need to be turned on and the MAC address for the desired extension account will need to be set up. Instructions using this method being on page 353.

- **Mass deployment ("auto provisioning")**: This method, known as redirection service, allows for touch-free, WAN-based plug and play and can be used for a large deployment of phones. You can arrange to have the MAC addresses of your phones provisioned to a setting URL that reflects your snom ONE. This way, when the phone boots up, the DHCP server will tell the phone your snom ONE's IP address, as well as other information. The redirection service requires a special arrangement with snom (mass deployment is discussed in more detail on page 354).
- **Manual setup**: This method is done by accessing the phone through a web browser. You will need to configure the phone's HTTP client information and the **Settings URL** setting so that the phone knows where the snom ONE is. Once the phone has logged into the system, the snom ONE will know which configuration files to send down to the phone (see page 331).

Plug and Play Checklist

Many snom ONE settings can be downloaded into the phone when the phone requests the configuration files. It is best to configure these settings ahead of time, so use this section as a preparatory checklist when preparing a phone for plug and play.

Configuring the Administrator Settings

To configure administrator settings for plug and plug, complete the following steps:

1. Go to **Admin** > **Settings** > **PnP**.

2. Scroll down until you see the **snom** settings.
3. Choose a transport layer from the available choices: UDP, TCP, or TLS.
4. If you have snom 300 phones and would like to customize them, you have the option to statically configure buttons 3 through 6, as shown in Figure 20-1.
5. You can also select the firmware version you would like to have running in the phone. If your firmware is newer than what is shown on the screen, you will need to get a matching version from snom's website; otherwise, the phone will be downgraded. You can also copy the firmware to a web server of your choice and even drop it in the `snomONE/html` directory so the system can serve it.

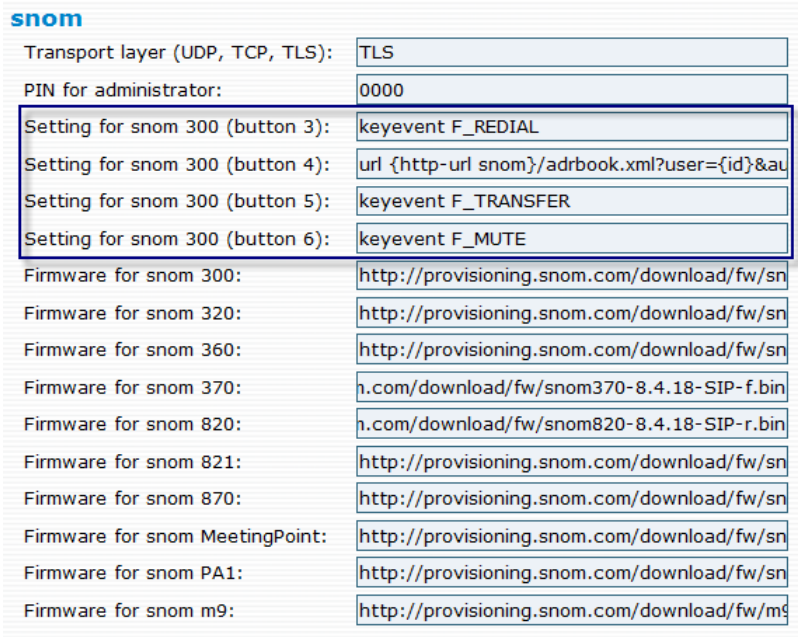


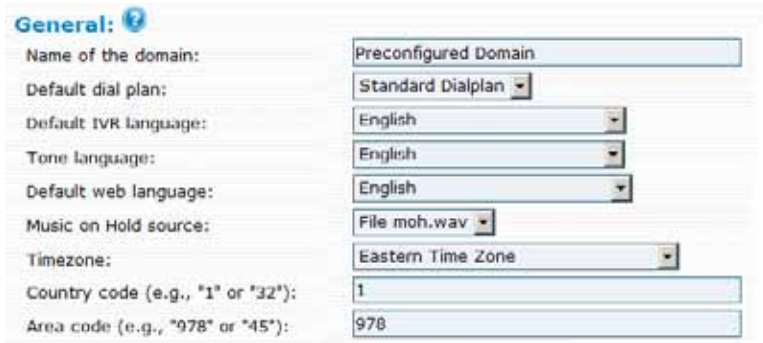
Figure 20-1. snom Plug and Play Settings

Configuring the Domain Settings

To configure the domain settings for plug and plug, complete the following steps:

1. Go to the **Domains** tab, click the domain, then click the **Settings** tab.

2. Choose default IVR and web languages, a time zone, and country and area codes.



- The IVR language influences the voice prompts of the voicemail system.
- The web language is used on the web interface pages.
- The time is reflected on the telephone display and in voicemail/email. It is also used in auto-generated reports, such as CDRs and status reports.
- The country and area codes affect the formatting of address book phone numbers.

3. Scroll to the bottom of the page to **Provisioning Parameters**, and select a default dial plan scheme.

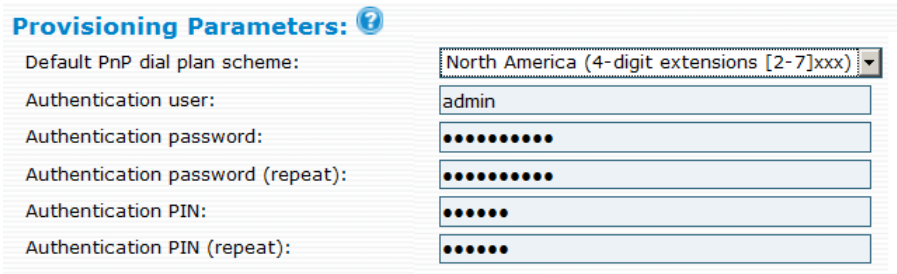
- The dial plan scheme tells the phone when to begin dialing, and numerous schemes are available (see page 107). If you want to customize the dial plan scheme, you can overwrite the `http://localhost/snom_3xx_dialplan_usa2.xml?model=snom320` file (where `localhost` is the FQDN or IP address of your snom ONE, and `snom_3xx` is the model of your phone, e.g., snom820, snom 870, etc.). Enter the URL into a browser, then download the file. Once you have made the necessary changes, place the modified version into the `html` directory. When snom ONE looks for the file, it will look in that directory before looking on the server.

Creating an Authentication Password

The authentication password setting allows administrators to provision phones and log into a phone's web interface remotely. This setting enables administrators to use identical usernames and passwords for all devices in a domain, simplifying the authentication process from the GUI of the phone. The password will bypass users' passwords (the web interface passwords), so users will not be able to use their passwords; hence, this setting can be used to keep users out of the phone's web interface and prevent them from inadvertently changing anything. When accessing the user's extension from the GUI of the phone, the format extension@domain is still required. The default username is `admin`, and the default password is `password`.

To set the **Authentication Password** setting, complete the following steps:

1. Go to **Domains**, click the domain, then click the **Settings** tab.
2. Scroll to the bottom of the page until you see **Provisioning Parameters**.
3. Enter a user name and password.



Setting up the Domain Address Book

Domain address books can be used by all extensions on the domain, and users can upload them into their phone (see page 426 for more on address books). Domain address books can be created through CSV files (instructions are provided in Appendix A).

Configuring the Button Profiles

This section allows you to create button profile(s) and assign them. Not all users will need the same button profile, so you may want to set up multiple profiles (see Chapter 19). If configuring a button for the busy lamp field (BLF), the **Watch the calls of the following extensions** setting (in the user's extension account) will need to list the extension(s) that will be monitored, and the **Permissions to monitor this account** setting (for the extension being monitored) will need to be set in order to allow for the monitoring.

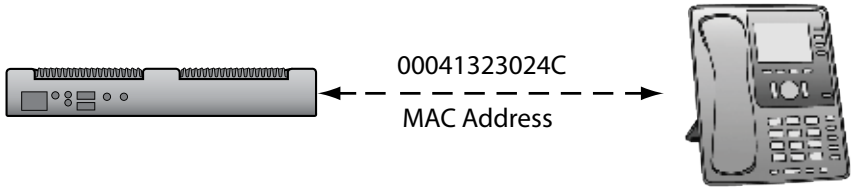
Creating the Extension(s)

The MAC address is an important setting when preparing a LAN-based extension for plug and play.

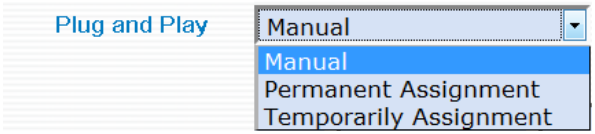
Important: WAN-based provisioning relies on login information rather than on MAC addresses, so if you are preparing WAN-based extensions for plug and play, you can skip this section.

The MAC address is the phone's unique hardware number and is used to identify the phone to snom ONE. It is a 12-digit hexadecimal number located on the back of the

phone and is written in the following format: `MMMMMMSSSSSS`, where `MMMMMM` represents snom's ID number and `SSSSSS` represents the serial number that snom assigned to the phone.



The snom ONE system needs to know how to associate the phone's MAC address with an extension. What determines this association is the **Plug and Play** setting located in the user's account. Three different options are available: manual, permanent assignment, and temporary assignment. These methods are detailed in Table 20-2.



Once you have selected a method, you will need to go to the extension account you want to associate the phone with and modify the **Bind to MAC Address** setting (see page 152). Populate the field with either the phone's MAC address, a star (*), or a question mark (?) (see Table 20-2 for syntax details). To get the MAC address of the phone, press the question mark (?) key. It will be displayed on the telephone display.

Table 20-2. Plug and Play Methods

Method of Plug and Play	Use Case Scenario	How it's Used
Manual	Setting up a few phones	The manual mode allows you to permanently set the MAC address in the extension account. This will bind the registration to a specific phone (see **Bind to MAC Address** on page 170). The MAC address can be used in multiple extensions, and multiple MAC addresses can be assigned to the same extension. This allows for users to have multiple phones. (Use a space to separate the MAC addresses.)
Permanent Assignment (*)	Deploying phones in a specified order in a large office	This mode allows you to easily assign MAC addresses to a large number of extensions. For example, rather than entering 100 different MAC addresses into separate user accounts, you can use the star symbol (*) to expedite the process. The system will assign a permanent extension to each phone once it boots up and requests a configuration from the system. The system will remember the MAC address of the phone and from that point on, the extension number will be used exclusively for that phone. This mode requires that a star (*) be used in the **Bind to MAC Address** field.
Temporary Assignment (?)	Setting up phones at trade shows, class rooms, etc.	The temporary assignment mode simplifies preparation when setting up at trade shows and for classroom training sessions. When this mode is used, the system will not remember which phone had been assigned to which extension. A phone might receive a new extension number every time it boots up. (As long as no other user agent is registered to a particular extension, the extension will be available for plug and play.) This mode requires that a question mark (?) be used in the **Bind to MAC Address** field.

If you are creating extensions using CSV files, the options shown in Table 20-2 can still be used. For the parameter, use `mac` and for the value, use the syntax that is indicated in the table.

Performing Plug and Play

DHCP, Option 66

This method can be used only if you have a DHCP server that supports option 66. You do not need to rely on multicast. Once you have set option 66 with the IP address of snom ONE, the DHCP server will be able to tell the phone where snom ONE is.

Note: If the phone was configured against a different location/snom ONE, you will need to reset the phone (see **Resetting the Phone** on page 359).

Preliminary step: If you have multiple snom ONE systems on the network, turn off the **Listen to sip.mcast.net** setting in the snom ONE web interface (**Admin** > **Settings**). Changing this setting requires a system restart.

1. Set up the MAC address of the phone for the desired extension account. To get the MAC address of the phone, press the question mark (?) key. It will be displayed on the telephone display. (This does not work for snom 300 phones; refer to your user guide.)

2. Connect the Ethernet cable to the phone, and power up the phone.

   When the phone reboots, it will get the IP address from the DHCP server (it may also get the TFTP server address). The phone will multicast the SUBSCRIBE message with its MAC address, vendor information, model information, and the version number. The system looks up the vendor information, model information, and version information of the phone from the message with the PnP configuration data (from the built-in `pnp.xml` file). If a match is found, the system will send the NOTIFY with the "Settings URL" file for the snom phone in the message body.

   Example: `https://192.168.1.109:443/provisioning/snom320.htm`. This file contains a list of files that are needed for the operation of the phone. Once the phone receives this file, it will send a request for each of the

files that are in the `snom320.htm` file (see Table 19-3). The snom ONE will generate these files and then send them to the phone based on the original SUBSCRIBE from the phone. The content of these files is controlled by the templates that are built into the binary of the system.

Table 20-3. Provisioning Files Requested by Phone

Settings	Provisioning Files
Provisioning file	`http://<pbx address>/provisioning/snom320.htm`
Firmware	`http://<pbx address>/provisioning/snom_3xx_fw.xml?model=snom320`
Password	`http://<pbx address>/provisioning/snom_3xx_phone.xml?model=snom320`
Dial plan scheme	`http://<pbx address>/provisioning/snom_3xx_dialplan_usa2.xml?model=snom320`
Buttons	`http://<pbx address>/provisioning/snom_3xx_fkeys.xml?model=snom320`
Web language	`http://<pbx address>/provisioning/snom_web_lang.xml?model=snom320`
Phone language	`http://<pbx address>/provisioning/snom_gui_lang.xml?model=snom320`
Custom settings	`http://<pbx address>/tftp/snom_320_custom.xml`

SIP SUBSCRIBE (Multicast)

This method is limited to environments with a single snom ONE. It is generally used in LANs, as multicast typically does not traverse routers. It requires configuration on the phone and is not supported if the phone is connected remotely (over the public Internet).

Note: If the phone was configured against a different location/system, you will need to reset the phone (see **Resetting the Phone** in this chapter).

1. From the web interface, click **Admin** > **Settings**, then scroll down to **SIP Settings**.

2. Turn on the **Listen to sip.mcast.net** setting. (*Note*: Changing the **Listen to sip.mcast.net** setting requires a system restart.)

3. Set up the **MAC address** of the phone for the desired extension account. To get the MAC address of the phone, press the question mark (?) key. It will be displayed on the telephone display. (If you have a snom 300, refer to your user guide for instructions on getting the MAC address.)

4. Connect the Ethernet cable to the phone, and power up the phone.

   When the phone reboots, it will get the IP address from the DHCP server (it may also get the TFTP server address). The phone will multicast the SUBSCRIBE message with its MAC address, vendor information, model information, and the version number.

   The system looks up the vendor information, model information, and version information of the phone from the message with the PnP configuration data (from the built-in `pnp.xml` file). If a match is found, the system will send the NOTIFY with the "Settings URL" file for the snom phone in the message body.

   Example: `https://192.168.1.109:443/provisioning/snom320.htm`. This file contains a list of files that are needed for the operation of the phone. Once the phone receives this file, it will send a request for each of the files that are in the `snom320.htm` file (see Table 19-3). The snom ONE will generate these files and then send them to the phone based on the original SUBSCRIBE from the phone. The content of these files is controlled by the templates that are built into the binary of the system.

Mass Deployment

Mass deployment (also known as "redirection service") allows for touch-free, WAN-based plug and play and is ideal for a large deployment of phones. To use this service, you will need to contact snom and have the MAC addresses of your phones provisioned to a setting URL that reflects your snom ONE.

By default, when the phone boots up for the first time, it contacts the snom server for its software updates (the setting URL is defaulted to www.snom.com), but once the setting server has been pre-programmed to redirect the phone to a different server (e.g., pbx.itsp.com), it will tell the phone the location of your snom ONE's IP address. The configuration files will be created in real time and will be sent to the phone using one of three protocols: HTTP, TFTP, or HTTPS.

The terms and conditions of snom's redirection service is detailed on the snom wiki (**wiki.snom.com**). Download the document, fill it out and sign it, then scan it and send it back to redirection@snom.com as a PDF attachment. You can also contact your nearest snom headquarters and send the contract by fax or mail. snom will contact you by e-mail to provide you with the necessary credentials.

Manual Method (HTTP)

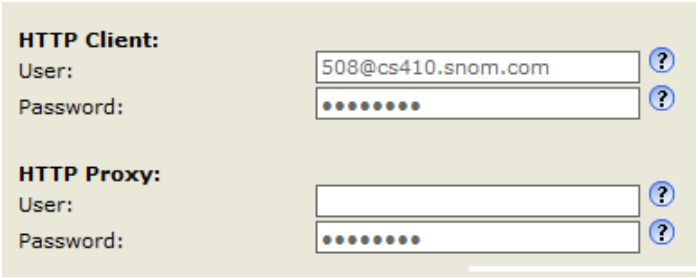
This method of plug and play can be used for phones in either a LAN (internal) or WAN (remote) environment. When used in a LAN environment, you need to set up the MAC address for the extension(s). This is done when you first **create the extension** (see the plug and play checklist in this chapter). When this method is used in a WAN environment, you will be able to use login information to authenticate the account, and all configurations will be made from the GUI of the phone.

Preliminary step: If you have multiple snom ONE's on the system, turn off the **Listen to sip.mcast.net** setting in the web interface (**Admin** > **Settings**). Changing the **Listen to sip.mcast.net** setting requires a system restart. You can do this by either restarting the computer, right-clicking **My Computer** and clicking **Manage** (choose **Service Applications** from the right pane), or by entering `net start snomone` from a command prompt.

1. Power up the phone.
2. Log in to the web interface of the snom phone by entering the phone's IP address into a web browser.
3. Click **Advanced** from the left-hand section of the screen.

4. Click the **QoS/Security** tab.

5. Scroll toward the bottom of the page until you see the **HTTP Client** information.



Note: The **HTTP Server** section contains user name/password information that is needed to log in to the phone using a web browser. After PnP, the system will configure this section with information from **Domain** > **Settings** > *Authentication User* and **Domain** > **Settings** > *Authentication Password*.

6. For **User**, enter the extension number of the phone. (If the phone had been registered to another extension and was not reset, you can delete the existing extension and enter a new extension.)

   Note: In multi-domain environments, the username must contain the extension and the domain (e.g., extension@domain).

   Note: The snom 870 requires the following format (there is no @ support):

   ```
   508;domain=sip.itsp.com
   ```


   The domain does not have to be a fully qualified DNS domain. The system will first identify the domain and then look for the extension within the domain. If found, it will request the **HTTP Authentication** details.

7. For **Password**, enter the extension level web password. The **Authentication User/Password** setting (see also the plug and play checklist) allows the administrator to create identical usernames and passwords for all devices in a domain.
8. Click **Save**.
9. Click the **Update** tab.
10. Set **Update Policy** to **Update automatically**.
11. Set **Settings URL** to `http://<PBX address>/provisioning/<snom820.htm>`, where `<PBX address>` can be the IP address or the FQDN of the PBX server, and `snom820.htm` should be replaced with the correct phone model (`snom360.htm`, `snom370.htm`, etc.).

    Important: Be careful when entering the text for the **Settings URL** setting. Plug and play will not work if the syntax is not entered exactly as indicated above.

12. Set **PnP Config** to **on** if the extension is in a LAN environment. For WAN, turn this setting to **off**.

Figure 20-2. Setting URL for the snom 820

13. Click **Save**.
14. Reboot the phone when prompted.
15. Click **Yes** to confirm that you want to reboot.

    During the reboot process, the phone will contact snom ONE and request the `snom820.htm` file with the authentication information that was set during Steps 6 and 7. The system will verify the authentication information and, if valid, will generate and send the requested file. Once the phone receives the file, it will send a request for each of the files that are in the `snom820.htm` file (Figure 20-3). The system will generate these files and send them to the phone based on the request from the phone. The content of these files is controlled by the templates that are built into the binary of snom ONE.

```
Setting server received via DHCP option 66: 192.168.1.251
Fetching URL: tftp://192.168.1.251/snom820.htm
Tftpclient: Request succeeded!
read_xml_settings: found setting-files XML header
read_xml_settings: found one byte encoding: 1
read_setting_file_list: added URL: http://192.168.1.251:80/provisioning/snom_3xx_fw.xml?mode
read_setting_file_list: added URL: https://192.168.1.251:443/provisioning/snom_3xx_phone.xml
read_setting_file_list: added URL: https://192.168.1.251:443/provisioning/snom_3xx_dialplan_
read_setting_file_list: added URL: https://192.168.1.251:443/provisioning/snom_3xx_fkeys.xml
read_setting_file_list: added URL: https://192.168.1.251:443/provisioning/snom_web_lang.xml?
read_setting_file_list: added URL: https://192.168.1.251:443/provisioning/snom_gui_lang.xml?
read_setting_file_list: added URL: https://192.168.1.251:443/tftp/snom_820_custom.xml
Conf setup: found xml style settings
```

Figure 20-3. Log File for snom 820

Resetting the Phone

If you have a phone that has been registered in the past or if are having trouble going into the phone GUI, you will need to reset the phone's configuration. You can do this through either the web interface, the phone itself, or from the GUI of the phone.

Using the Phone

snom 300 and 320

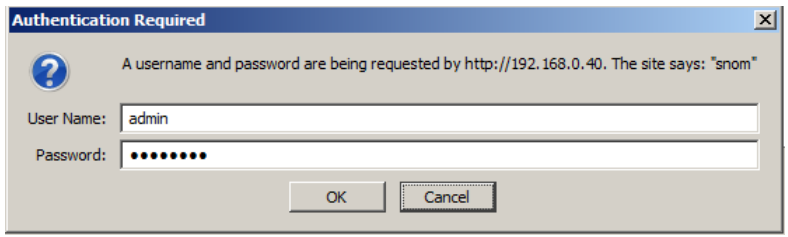
Warning: All current settings will be lost.

1. Use the bottom edge of the navigation wheel (↓) to navigate to **Configuration**. (You will need to press the ↓ key ten times.)
2. Press the right edge (→) of the navigation wheel once. You should see **Reset**.
3. Press the confirm key.
4. Enter the password (snom's default password is `0000`).

snom 360 and 370

Warning: All current settings will be lost.

1. Press the **Settings** key.
2. Use the bottom edge of the navigation wheel to navigate to **Maintenance**, then press the confirm key.
3. Navigate to **Reset Values**, then press the confirm key.
4. Enter the password (snom's default password is `0000`).



snom 820

Warning: All current settings will be lost.

1. Press the **Menu** key.
2. Use the bottom edge of the navigation wheel to navigate to **Maintenance**, then press the confirm key.
3. Navigate to **Reset Values**, then press the confirm key.
4. Enter the administrator password.

snom 870

Warning: All current settings will be lost.

Use one of the following methods:

1. Unplug the phone.
2. Press the hash key (#).
3. Plug the phone back in, keeping the # key depressed.
4. Continue pressing the # key until the Rescue Mode screen is displayed (approximately 18 to 20 seconds).
5. Once the Rescue Mode screen is displayed, press option 1 (Settings reset).

You can also use the phone display without unplugging the phone, but you will need to know the admin password (default is `0000`).

1. Tap from the phone display.
2. Select **Maintenance**.
3. Select **User Mode**.
4. Select **Administrator Mode**.
5. Enter administrator password.
6. Select **Reset Values**, then press the confirm key.
7. Wait for prompt.

Rebooting the Phone

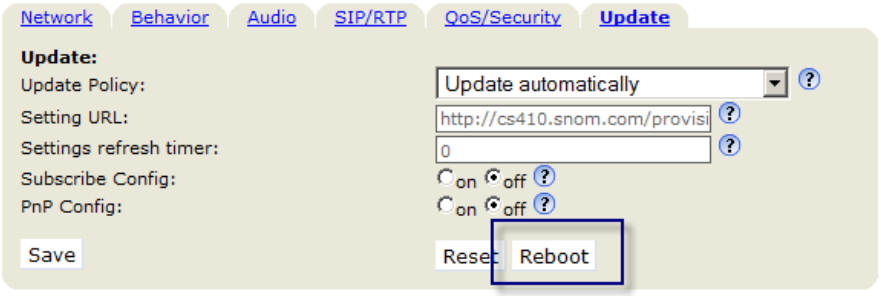
Using the Phone

From the phone, enter **#*.

Using the Phone GUI

1. Enter the IP address of the phone into a web browser.
2. Click **Advanced** from the yellow left-hand section of the screen.

3. Click the **Update** tab.
4. Click **Reboot**.



Updating the Firmware Via TFTP

Updating the firmware via TFTP (also known as flashing the phone) is intended for the initial setup of the phone and for situations when there is no other way to get the phone working again.

Download the Recovery Firmware

The first steps to flashing a phone include downloading the recovery firmware image and then placing it in the `snomone/tftp` directory. These steps are detailed below:

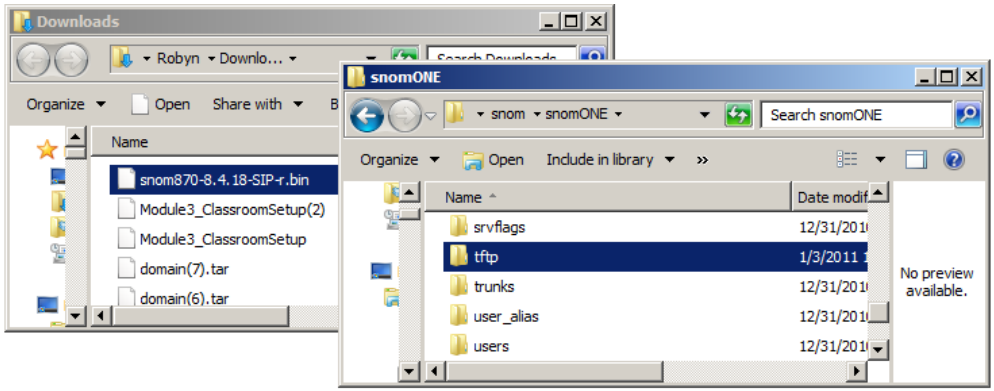
1. Go to `http://wiki.snom.com` and click **Firmware Guide** as shown below:

2. Click your phone model, then click the firmware version.

3. Click the recovery image.

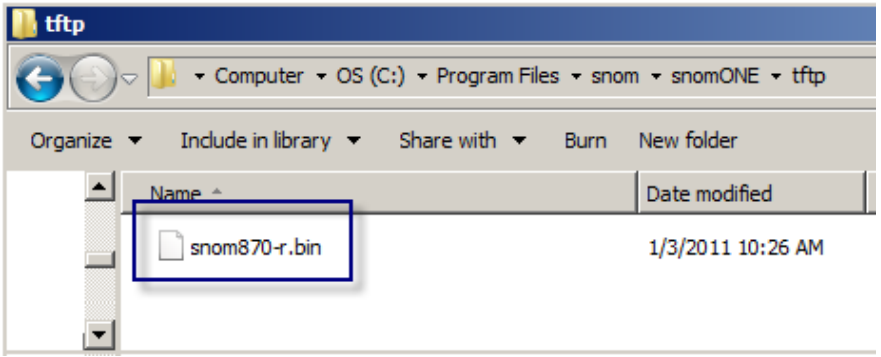
4. Click the download link, and save the file.

5. Move the file into the `snomone/tftp` folder (create a `tftp` folder you don't have one).



6. Rename the file `snomxxx.bin`, where `xxx` is the model number of the phone, e.g., `360` for the snom 360.

   Note: For the snom 820 and 870, the recovery firmware image must be renamed to include an "`r`" (e.g., `snom820-r.bin` for the snom 870).



TFTP Process

Once the `*.bin` file is located in the `snomone/tftp` directory, the phone needs to be configured so that it can fetch it from that location.

Note: Updating the firmware with the TFTP update application also erases the settings in the flash. This means that all previous settings are lost and the phone does not even know its own identity.

1. *For the snom 3xx series*, on booting up the phone, press any key when "To update by TFTP, press any key" is displayed. The TFTP update screen is displayed. If the TFTP update prompt is not shown, power cycle the phone.

   For the snom 8xx series, unplug the phone, then while pressing the # key, power the phone back up. Continue pressing the # key until you see the Rescue Mode screen.

2. Press 2 from the phone keypad, then enter the following information, followed by the confirm key each time:

   Note: If the phone and the tftp server are on the same subnet, only the IP address and the tftp server need to be entered.

   - IP-Addr: 192.168.0.32 (the phone)

- Netmask: 255.255.255.0
- Gateway: 192.168.0.1 (the router)
- Server: 192.168.0.31 (the PC/laptop)

When successful, the TFTP update application begins to erase the flash and then rewrite the image. This process takes approximately 1 minute.

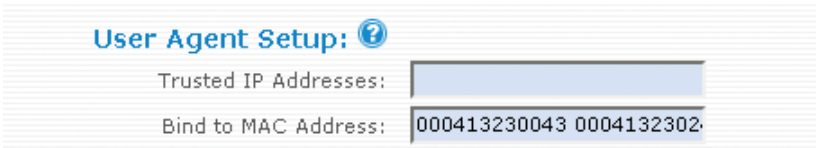
If the download process fails for any reason, the CRC check will also fail and the TFTP update application will refuse to erase the application firmware flash section. Problems can occur when you are using certain types of NICs:

- Onboard NVIDIA nForce Networking Controller
- ASRock AM2NF3-VSTA Mainboards with nForce-3 Chipset under Windows XP Pro

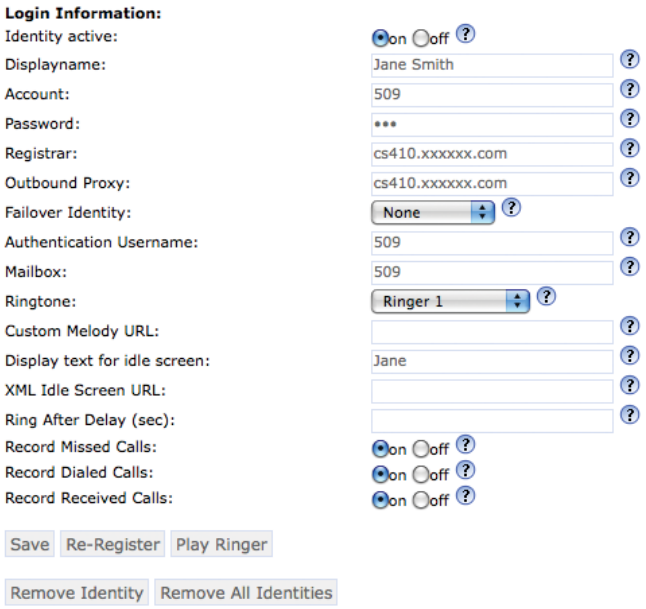
Registering Numerous Extensions to One Phone

Registering multiple identities to a single phone can be useful in cases when the phone is being used to answer calls for numerous companies. Each identity has its own extension, and the extension can be configured to a system that is either local or remote.

1. Enter the MAC address of the phone into the **Bind to MAC Address** field of the new extension, as shown below (**Registrations** tab).



2. Reboot the phone by entering **#* from the telephone key pad. The phone will reboot and reprovision itself as it counts down from 20 to 1.
3. Enter the IP address of the phone into a web browser.
4. Click **Settings** > **Identity** (at the bottom left of the screen).



5. Populate the screen using the following information:
   - **Identity Active:** Enable this setting
   - **Display name:** Enter the name that will be used for the account.
   - **Account:** Enter the additional extension number.
   - **Password:** Enter the SIP password of the additional extension.
   - **Registrar:** Enter the domain name of the system.
   - **Outbound Proxy:** Specify the IP or DNS address of the registrar/proxy where you want to register this account. After a successful registration, the registrar knows how to reach this specific identity and can route requests (e.g., incoming calls) from other registered parties to this phone. If the extension is local, enter the IP address of the system; otherwise, enter a domain name.
   - **Failover:** This field allows you to enter an extension where calls will be sent if the extension is down.
6. Click **Save**.
7. Click **Re-Register**.

The telephone display will reflect the new identity:

Overriding Plug and Play Defaults

Plug and play default settings can be modified using a few different methods. The first method is to use the **Admin** > **PnP** tab, which allows you to modify only a small number of settings. To make large-scale custom configurations, you will need a customized XML file.

Changing Default Settings from Admin > Settings > PnP

This section shows you how to manually change plug and play settings using the **Admin** > **PnP** tab. The only changes that you can make using this method are the transport layer, the password of the snom phone, some of the buttons on the snom 300 phone, and the firmware versions. Once the changes have been made and the phone has been rebooted, the phone will request the configuration files from the server and the changes will take effect.

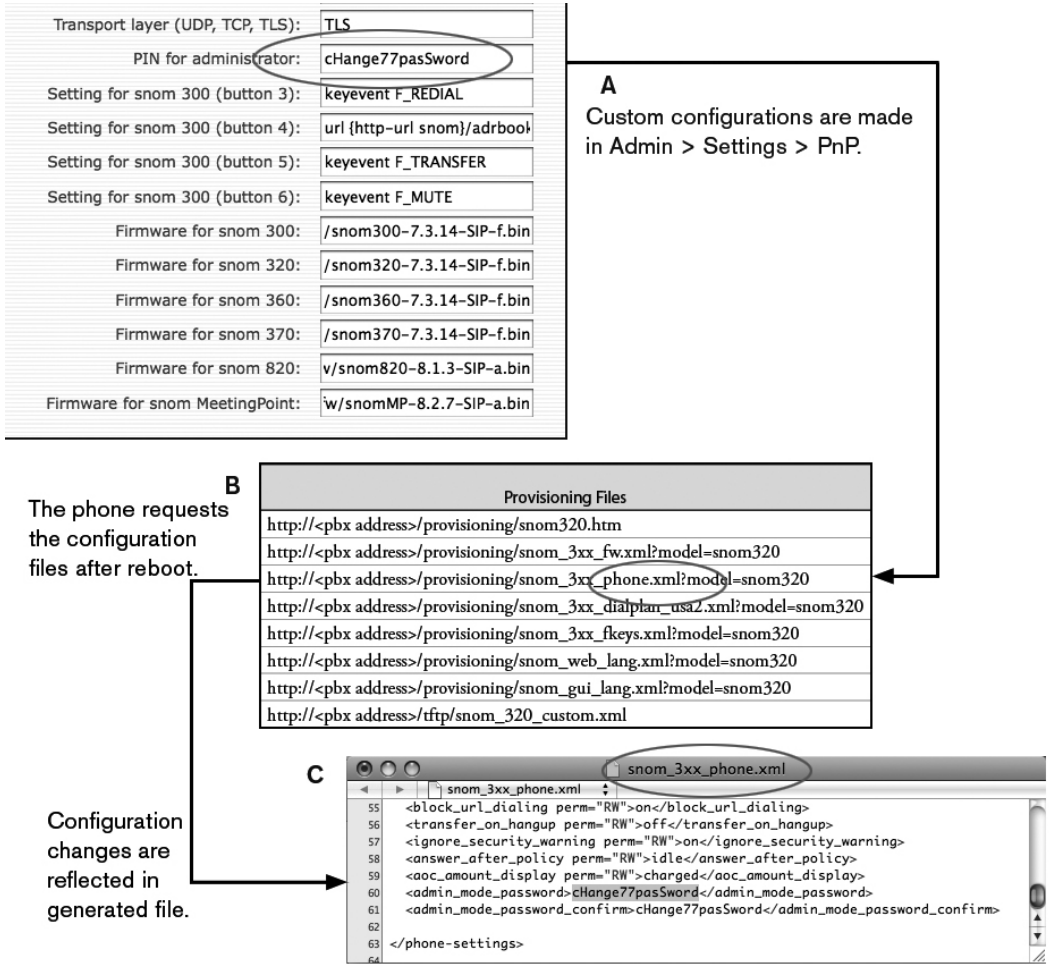
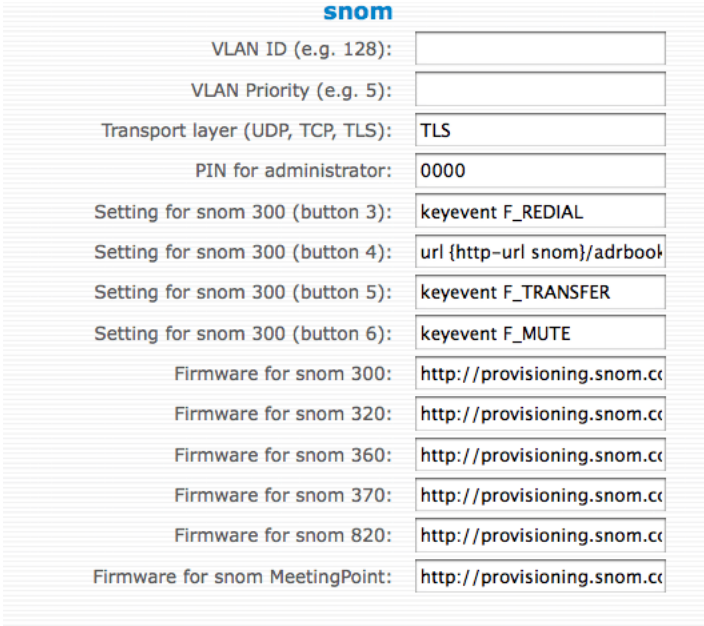


Figure 20-4. Overriding Default Plug and Play Settings (Using Admin > PnP)

To make any of the custom settings shown in Figure 20-4(A), use the following steps:

1. Go to **Admin > Settings** > **PnP** and scroll down to the **snom** settings.



2. Make the necessary configurations. (The button settings are for snom 300 phones only.)
3. Click **Save**.
4. Reboot each phone on the domain by going into the **Registrations** tab of each phone and clicking **check-sync**.

The files within each user's account will reflect the changes.

Changing Default Settings Using a Customized XML File

snom phones have hundreds of settings that are used to give the phone its functionality. Not all these settings are currently part of plug and play. However, through the use of a customized file, you can integrate missing settings into plug and play. Before doing any

customization, read through these next few pages so that you have a thorough understanding of how customized files reach the phone.

Generated Files and Where They Come From

When the phone contacts the system for its configuration files during plug and play, the system creates a directory for each extension, so that it will have a place to put the files. The directory is called `generated` and the files are shown in Figure 20-5. The full path on Windows is `Program Files\snom\snomONE\generated\pbx.company.com`, and on the Mac it is `usr\Applications\pbx\generated\pbx.company.com`.

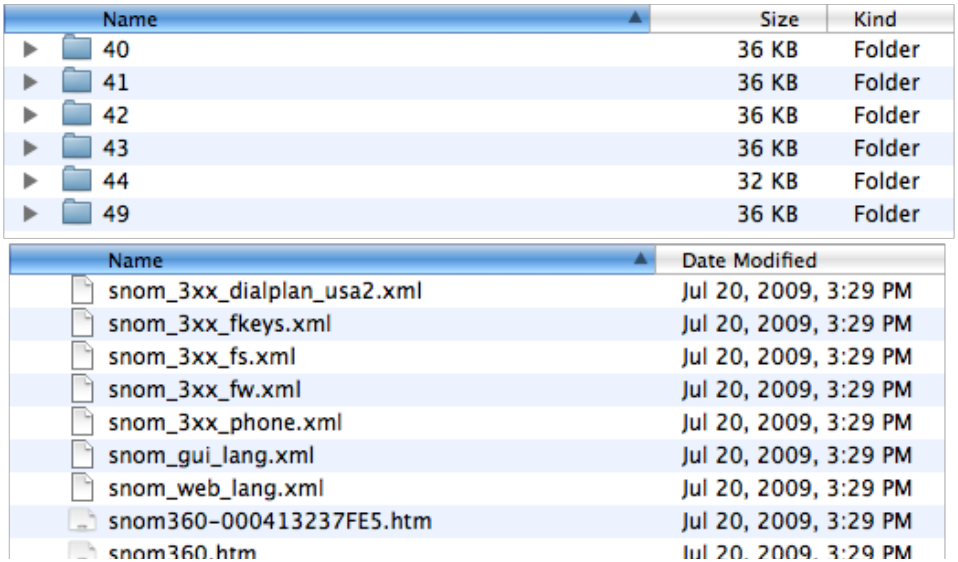


Figure 20-5. Directory Structure of Extensions on Domain

The files are generated from templates that exist in the binary (inaccessible files) of the snom ONE. When the phone boots up, it looks at the files in the `generated` directory and will take on the settings that are represented by those files. By default, the only files it sees are the files shown in Figure 20-5. However, by placing `snom_3xx_custom.xml` (`xxx` must reflect the phone model) into an `tftp` directory (which you must create), the phone will see those settings as well. Figure 20-6 provides an abbreviated overview of how plug and play works and the role that generated files play. After

snom ONE has sent the phone its `snomxxx.htm` file (Step 4 below), the phone will request its configuration files. At this point, snom ONE will process the plug and play settings and compile them into generated files, which are received by the phone once it reboots.

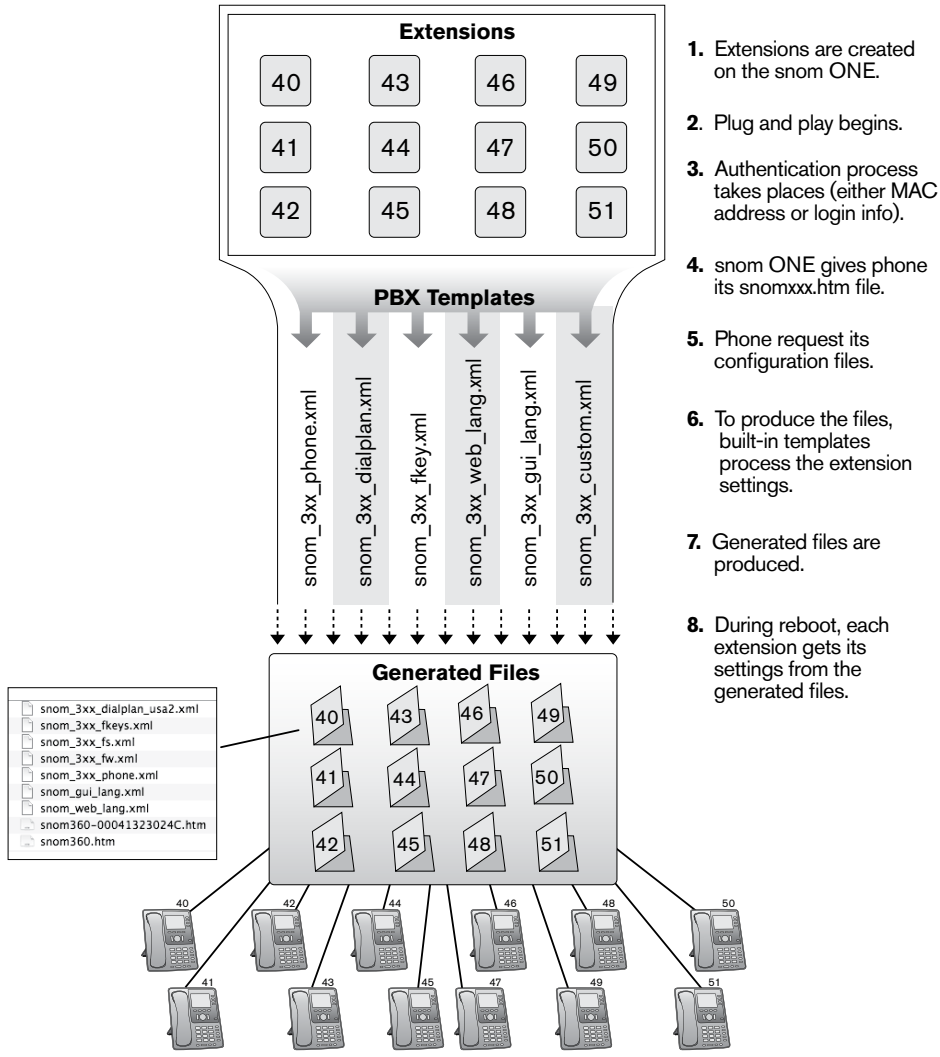


Figure 20-6. Generated Extension Files

Figure 20-7 shows one of the template files (`snom_3xx_phone.xml`) that the system uses to create one of the generated files. Though you cannot access this file, it is important to notice the structural syntax that is used in the file because the customized file will need to follow a similar structure.

```
<?xml version="1.0" encoding="utf-8" ?>
- <phone-settings>
    {loop-start 1}
    <user_active idx="{lc}" perm="RW">on</user_active>
    <user_realname idx="{lc}" perm="RW">{display-name}</user_realname>
    <user_idle_text idx="{lc}" perm="RW">{account}: {display-name}</user_idle_text>
    <user_name idx="{lc}" perm="RW">{account}</user_name>
    <user_pname idx="{lc}" perm="RW">{account}</user_pname>
    <user_host idx="{lc}" perm="RW">{domain}</user_host>
    <user_pass idx="{lc}" perm="RW">{sip-pass}</user_pass>
    <user_mailbox idx="{lc}" perm="RW">{account}</user_mailbox>
    <user_srtp idx="{lc}" perm="RW">on</user_srtp>
    <user_auth_tag idx="{lc}" perm="RW">on</user_auth_tag>
    <user_symmetrical_rtp idx="{lc}" perm="R">off</user_symmetrical_rtp>
    <user_auto_connect idx="{lc}" perm="RW">off</user_auto_connect>
    <user_descr_contact idx="{lc}" perm="RW">off</user_descr_contact>
    <user_xml_screen_url idx="{lc}" perm="RW" />
    <user_proxy_require idx="{lc}" perm="RW">buttons</user_proxy_require>
    <user_outbound idx="{lc}" perm="RW">{outbound-proxy snom_transport}</user_outbound>
    <codec1_name idx="{lc}" perm="RW">9</codec1_name>
    <codec2_name idx="{lc}" perm="RW">0</codec2_name>
    <codec3_name idx="{lc}" perm="RW">8</codec3_name>
    <codec4_name idx="{lc}" perm="RW">2</codec4_name>
    <codec5_name idx="{lc}" perm="RW">3</codec5_name>
    <codec6_name idx="{lc}" perm="RW">18</codec6_name>
    <codec7_name idx="{lc}" perm="RW">4</codec7_name>
    <codec_size idx="{lc}" perm="RW">20</codec_size>
    <stun_server idx="{lc}" perm="R" />
    <user_dtmf_info idx="{lc}" perm="R">off</user_dtmf_info>
    <user_server_type idx="{lc}" perm="R">pbxnsip</user_server_type>
    <user_subscription_expiry idx="{lc}" perm="R">3600</user_subscription_expiry>
    <stun_binding_interval idx="{lc}" perm="R" />
    <record_missed_calls idx="{lc}" perm="RW">on</record_missed_calls>
    {loop-end}
    <dkey_snom perm="RW">url {http-url snom}/missed.xml?user={id}&auth={webhash}</dkey_snom>
    <dkey_directory perm="RW">url {http-url snom}/adrbook.xml?user={id}&auth={webhash}</dkey_directory>
    <dkey_menu perm="RW">url {http-url snom}/menu.xml?user={id}&auth={webhash}</dkey_menu>
    <timezone perm="RW">USA</timezone>
    {ifn_button dnd none}
    <dnd_on_code perm="RW">{starcode code_dnde}</dnd_on_code>
    <dnd_off_code perm="RW">{starcode code_dndd}</dnd_off_code>
    {fin_button dnd none}
    <utc_offset perm="RW">{tz gmt-offset}</utc_offset>
    <dst perm="RW">{tz dst-snom}</dst>
    <http_user perm="RW">{admin-user}</http_user>
    <http_pass perm="RW">{admin-pass}</http_pass>
    <http_client_user perm="RW">{account};domain={domain}</http_client_user>
    <http_client_pass perm="RW">{web-pass}</http_client_pass>
    <with_flash perm="RW">off</with_flash>
    <language perm="RW">{enum extension lang_audio English sp=Espanol de=Deutsch fr=Francais nl=Nederland
      Italiano pl=Polski tr=Turkce}</language>
    <web_language perm="RW">{enum extension lang_audio English sp=Espanol de=Deutsch fr=Francais nl=Nede
      Dansk it=Italiano pl=Polski tr=Turkce}</web_language>
```

Figure 20-7. Sample of a Template File (snom_3xx_phone.xml)

Figure 20-8 shows an example of the generated version of `snom_3xx_phone.xml`.

snom_3xx_phone.xml

```
<?xml version="1.0" encoding="utf-8"?>
<phone-settings>
  <user_active idx="1" perm="RW">on</user_active>
  <user_realname idx="1" perm="RW">Fourty Zero</user_realname>
  <user_idle_text idx="1" perm="RW">40: Fourty Zero</user_idle_text>
  <user_name idx="1" perm="RW">40</user_name>
  <user_host idx="1" perm="RW">pbx.company.com</user_host>
  <user_pass idx="1" perm="RW"></user_pass>
  <user_mailbox idx="1" perm="RW">40</user_mailbox>
  <user_srtp idx="1" perm="RW">on</user_srtp>
  <user_symmetrical_rtp idx="1" perm="R">off</user_symmetrical_rtp>
  <user_auto_connect idx="1" perm="RW">off</user_auto_connect>
  <user_descr_contact idx="1" perm="RW">off</user_descr_contact>
  <user_xml_screen_url idx="1" perm="RW"></user_xml_screen_url>
  <user_proxy_require idx="1" perm="RW">buttons</user_proxy_require>
  <user_outbound idx="1" perm="RW">sip:192.168.1.102:5061;transport=tls</user_outbound>
  <codec1_name idx="1" perm="RW">9</codec1_name>
  <codec2_name idx="1" perm="RW">0</codec2_name>
  <codec3_name idx="1" perm="RW">8</codec3_name>
  <codec4_name idx="1" perm="RW">2</codec4_name>
  <codec5_name idx="1" perm="RW">3</codec5_name>
  <codec6_name idx="1" perm="RW">18</codec6_name>
  <codec7_name idx="1" perm="RW">4</codec7_name>
  <codec_size idx="1" perm="RW">20</codec_size>
  <stun_server idx="1" perm="R"></stun_server>
  <user_dtmf_info idx="1" perm="R">off</user_dtmf_info>
  <user_server_type idx="1" perm="R">pbxnsip</user_server_type>
  <user_subscription_expiry idx="1" perm="R">3600</user_subscription_expiry>
  <stun_binding_interval idx="1" perm="R"></stun_binding_interval>
  <record_missed_calls idx="1" perm="RW">on</record_missed_calls>
  <dkey_snom perm="RW">url http://192.168.1.102:80/snom/missed.xml?
user=1&amp;auth=a678fc152943f7d9bb30a9e2f164d9f4</dkey_snom>
  <dkey_directory perm="RW">url http://192.168.1.102:80/snom/adrbook.xml?
user=1&amp;auth=a678fc152943f7d9bb30a9e2f164d9f4</dkey_directory>
  <dkey_menu perm="RW">url http://192.168.1.102:80/snom/menu.xml?
user=1&amp;auth=a678fc152943f7d9bb30a9e2f164d9f4</dkey_menu>
  <dkey_dnd perm="RW">button dnd</dkey_dnd>
  <timezone perm="RW">USA</timezone>
  <utc_offset perm="RW">-18000</utc_offset>
  <dst perm="RW">3600 3.2.7 2:0:0 11.1.7 2:0:0</dst>
  <http_user perm="RW">40</http_user>
  <http_pass perm="RW"></http_pass>
  <with_flash perm="RW">off</with_flash>
  <language perm="RW">English</language>
```

Figure 20-8. Sample of a Generated File (snom_3xx_phone.xml)

Before you can create a customized file, you will need to know the XML element tags that have been reserved for each setting, as well as the parameters that can be used. You will find this information on the snom web site (Figure 20-9). (Once you have HTTP'd into a phone, click **Settings** at the bottom left part of the screen. The settings are listed

on the right side of the page.) You may also need the snom administrator guide for an explanation of parameter requirements.

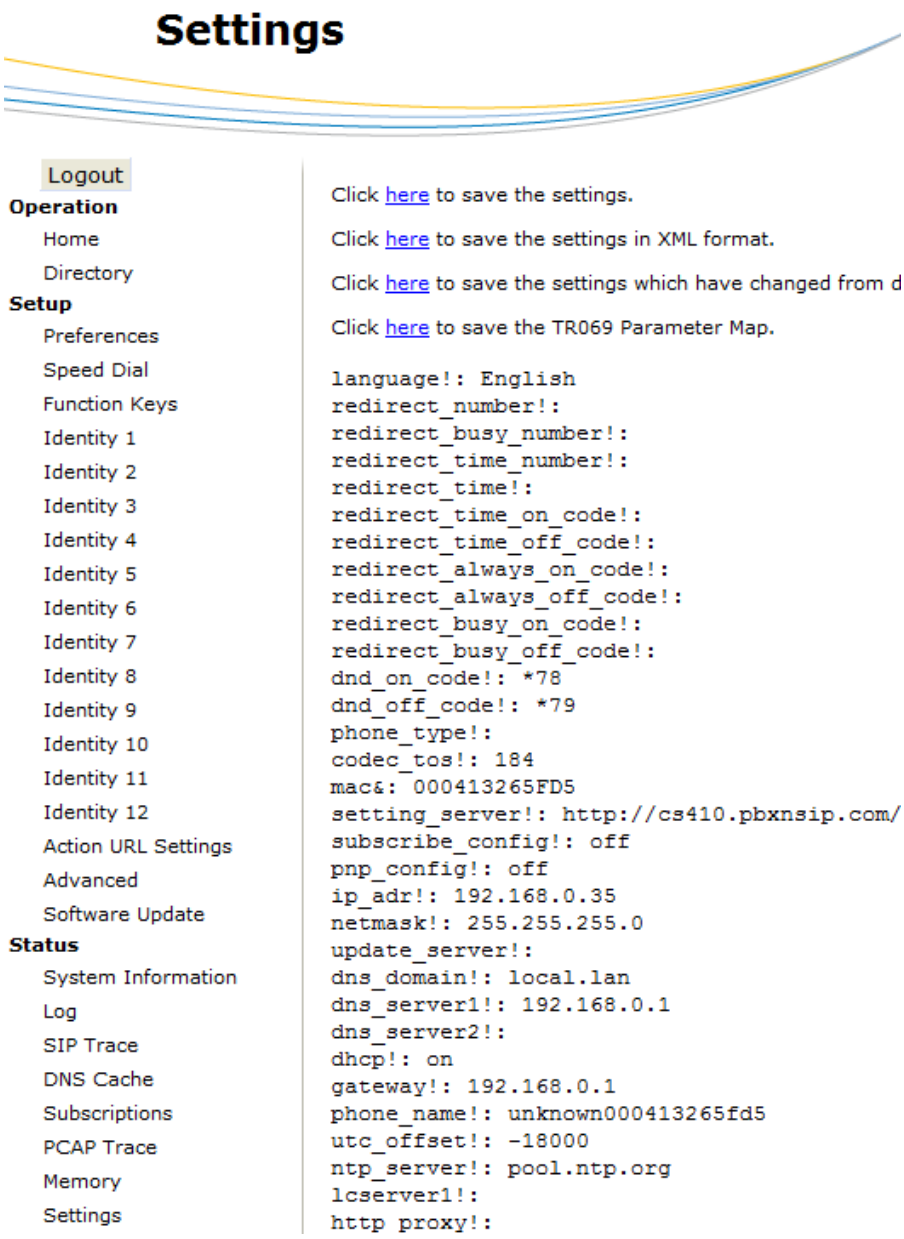


Figure 20-9. snom Phone Settings

When the settings are viewed in XML, the following document tree is displayed:

Figure 20-10. Document Tree of snom Phone Settings

Creating a Customized File

1. Create a directory named `tftp` on the system:

   Windows: `Program Files\snom\snomONE\tftp`

   Mac: `usr\Applications\pbx\tftp`

2. Create the customized file using an XML editor. Following are a few lines from a customized file (these settings are highlighted in Figure 20-10). The information that will be picked up by the phone is shown in bold.

   ```
   <?xml version="1.0" encoding="utf-8" ?>
   <settings>
    <phone-settings>
     <redirect_number>9781234567</redirect_number>
     <redirect_busy_number>6031234567</redirect_busy_number>
     <pnp_config>off</pnp_config>
   </phone-settings>
   </settings>
   ```

3. Save the file as `snom_xxx_custom.xml` (where `xxx` reflects the model of the phone; for example, `snom_320_custom.xml` for a snom 320).
4. Place the file in the TFTP directory you just created.

Once the phone reboots, it will pick up your customized settings.

Troubleshooting

Following are solutions for common plug and play issues:

Table 20-4. Troubleshooting

Issue	Notes	Resolution
Provisioning countdown issue: The phone was registered somewhere else, and you are trying to move the phone to a new extension.	The phone may be sending the old authentication information and the system will reject it.	Reset the phone.
Provisioning countdown issue: The phone tries the multicast SUBSCRIBE and the system ignores it.	This will happen if **sip.mcast.net** is turned off.	Turn on **sip.mcast.net** on the system. You can also try turning off the **Advanced** > **Update: PnP Config** on the phone and following the HTTP-based PnP process.
Provisioning countdown issue: The proper username and password combination have not been set.	This applies to the HTTP PnP method.	Properly match the username and password on both the snom ONE and the phone.
Provisioning countdown issue: Some SIP-aware routers are altering the messages.		Turn off the SIP awareness on the routers or replace the routers.
Multiple snom ONE instances are running on the same network.	This could inadvertently affect the multicast SUBSCRIBE-based PnP.	Verify who is responding to the phone's requests by looking at the phone log (or some type of network sniffer).
Username and password do not show up.	You may have a firewall issue.	

Issue	Notes	Resolution
Can't HTTP into the phone or unable to reset the password on the phone.	1. Copy the phone's firmware from the wiki.snom.com web site to the `tftp` directory of the snom ONE. 2. Modify the **PnP** tab of the snom ONE with the firmware version that was downloaded. 3. Rename it `snomxxx.bin`. 4. Reboot the phone. 5. Hit any key on the phone within 3 seconds, and then manually enter the IP address of the phone, the IP address of the snom ONE, the default gateway if the system is off from the network, and the subnet mask. 6. Click the checkbox. The phone should connect to the snom ONE and download the firmware and reset itself.	

Chapter 21

MUSIC ON HOLD

Music on hold (MoH) is recorded music that callers listen to while waiting on hold. It is used to avoid silence on the line and is used in several places of the system: when a call is on hold and when a caller is waiting in an agent group queue (see Chapter 11 for more on agent groups). The system allows three different source types for its music on hold: file, wave input, and RTP stream. These sources serve different purposes and are detailed below. The sources can be used in parallel in different locations on the same system.

- **Files:** The system can use one or more files for MoH. These files are read by the system on demand and are played in an endless loop. Files must be placed manually into the `audio_moh` directory of the system. Although files are loaded only once, long files will be read into memory and can consume a lot memory space. Keep in mind that each minute of the file will require about 1 MB of memory space, so a 7-minute file will take up about 6.7 MB (128 kbit/s * 7 * 60 seconds). After it gets past the initial hick-up (jitter), subsequent calls to the MoH file will be smooth.

  Format: Files must be in 8-kHz sampling frequency, and they should be in 16 bit per sample signed format. The format must be mono WAV. You may also use other formats (u-law and GSM), but these formats will have less audio quality and require more CPU performance.

- **Wave input:** In Windows, snom ONE can read MoH from an audio input jack, which is a convenient way to connect a CD, MP3 player, or a radio to the system. The disadvantage of this method is that only one external music source can be used.

  You can also internally loop the audio output of the local computer back to the audio input of the computer. This allows you to use an MP3 player run-

ning locally to provide a large number of MP3 files. However, we recommend keeping an eye on the memory usage of the MP3 player, as some players have memory leaks and slowly consume the memory of the computer.

Note: This feature is currently available only for Microsoft Windows-based operating systems. The appliance uses the RTP streaming mode for the audio input jack.

- **RTP stream:** Streaming RTP data is a popular way of providing music from external sources. As with a telephone conversation, the system receives the audio data in a standard RTP stream. Several external tools are available that are able to generate a compliant RTP stream. Because the system can have several RTP streams, you can use this method to generate different music on hold sources for the system.

  Format: The RTP stream must use G.711 encoding. No SIP signalling is involved with this method, and the system does not send RTP data back.

  Important: Be sure to specify the port on which the system should listen for RTP input (e.g., `42000`). This port must be available on the system. If you change the setting, you might need to restart the system service so that the change takes effect.

Setting up Music on Hold

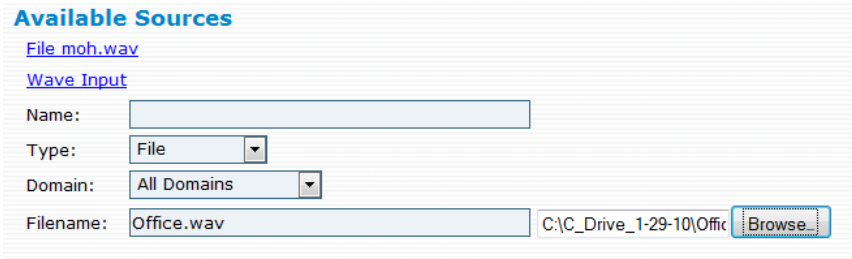
MoH sources are available to all domains on the system, so setup is done from the administrator level.

1. Navigate to **Admin** > **Settings** > **MoH**.

2. Populate the fields using the following information:

   - **Name**: Assign a name to the MoH source (this name will appear in the Available Sources list at the end of this exercise).
   - **Type:** From the dropdown, choose the type of MoH that you will be using.
   - **Domain:** From the **Domain** dropdown, select your domain.
   - **Filename:** This field depends on which type of MoH you are using:

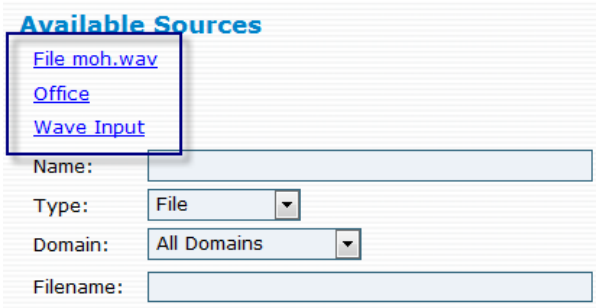
     File: If you are using files, upload the file by clicking **Browse**. (Once the file has been uploaded, it will automatically get filed in the `audio_moh` directory.)



     WAV Input: If you are reading MoH from an audio input jack, the **Filename** field will disappear.

     RTP Stream: If you are streaming RTP data, enter the port on which the system should listen for RTP input (e.g., `42000`). This port must be available on the system. If you change the setting, you might need to restart the system service so that the change takes effect.

3. Click **Create**. The new source will be listed as an available source.



4. To verify that the source has been added on the domain level, navigate to **Domain** > **Settings**. You should see the newly added source in the **Music on Hold Source** dropdown:

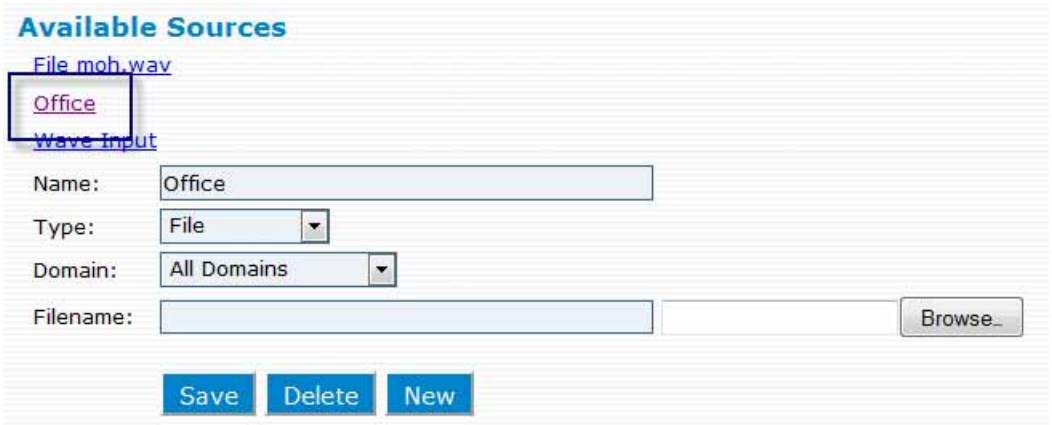
Once MoH has been created, it can be selected for use on a domain level within both the agent group and hunt group accounts.

Editing MoH Sources

Once you have created an MoH source, you can do the following:

- Change the name of the source.
- Change the domain(s) that will have access to it.
- Delete it from the list of available sources.

To edit a source, click the source link and make the changes in the form below it. Then click **Save**.

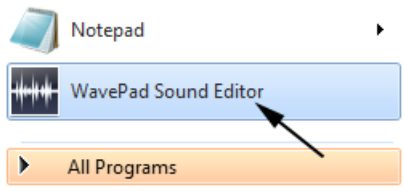


To delete a source, click the source link and click **Delete**.

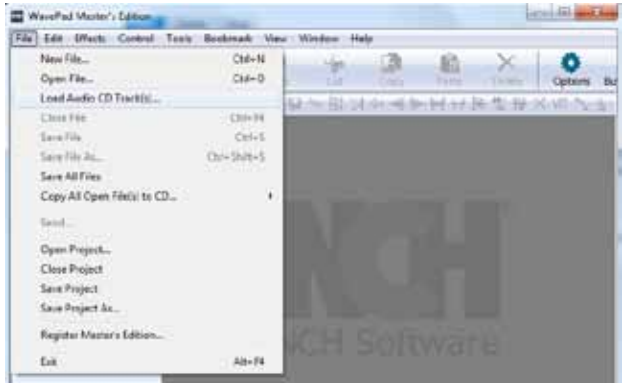
Creating WAV Files

Creating a WAV file from a CD is easy and can be done using most music player programs. These instructions were done using WavePad (freeware from www.nch.com).

1. Install WavPad on your computer.
2. Launch the program (**START** > **All Programs** > **WavePad Sound Editor**).



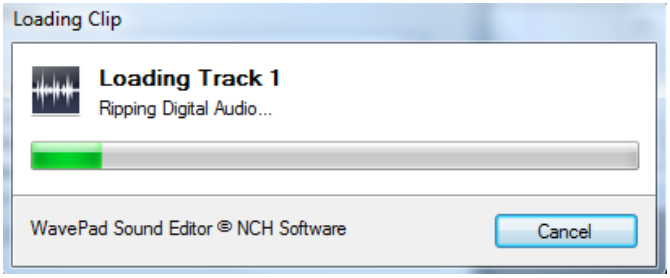
3. Put the CD into your CD-ROM drive.
4. Click **File** > **Load Audio CD Track(s)**.



5. Select the track you want to use and click **Load**.

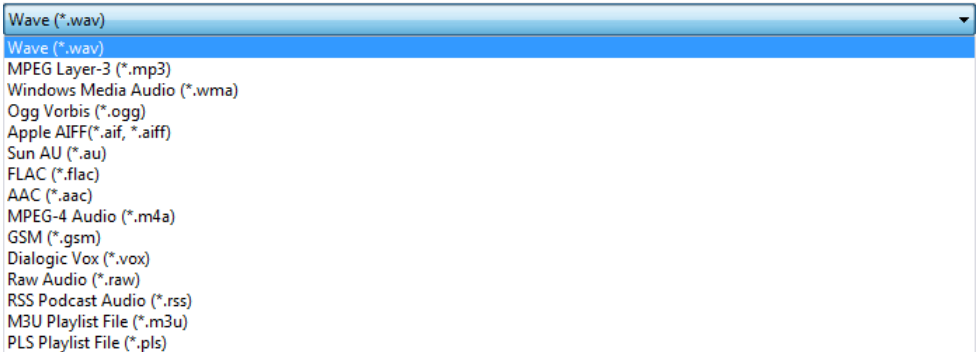
Load Audio CD Track(s)
CD-ROM Drive
D:\ PLDS DVD+RW DH
Refresh
Select Track(s)
Track
What Made You Say That
You Lay a Whole Lot of Love on Me
Dance With the One That Brought You
Still Under the Weather
God Ain't Gonna Getcha for That

The following screen will be displayed while the track is loading:



When the file has finished loading, you will see the following screen:

6. Click **Save File**.
7. Choose the .WAV format from the list if it's not selected by default.



8. Navigate to the `audio_moh` directory (`C:\Program Files\snom\snomone\audio_moh`), and save the file.

Configuring Paging/Music on Hold

The snom ONE Paging/Music on Hold application allows you to use a PC to stream audio from a music on hold input and play back audio on a paging output. This section details the installation and basic configuration of the application. The following conditions are assumed:

- You are running the application on the same system/PC on which you are running the system.
- You are running the system on a Windows PC equipped with a sound card.

snom phones, due to plug-and-play features, will automatically play back the audio stream. The system searches for the first MC paging account in the domain and automatically configures the phones to play back that audio stream. This is valid for version 7.x only; later versions have multiple MC streams and will need to be configured to specify which phones are permitted to listen to a particular stream.

Download and Installation

Go to wiki.snomone.com and download and install the Paging and MoH application.

The installation will create the application as a service. The installer will also copy a `pagmoh.xml` file to the installation folder. This file will contain the default settings that are used by the application. These defaults are listed below:

- Paging port = 5000
- MoH port = 6000
- Codec = μ law
- Service name = pagmoh

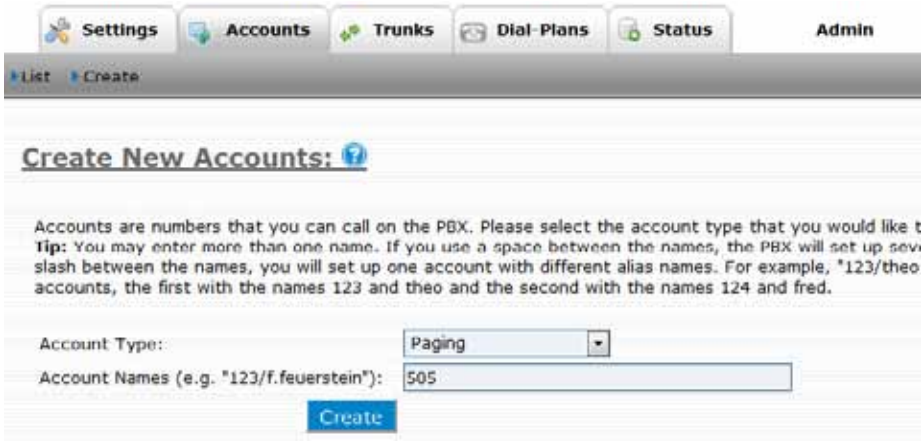
You can edit this file so that different ports may be used. After changing any values, restart the service.

Setting up Paging

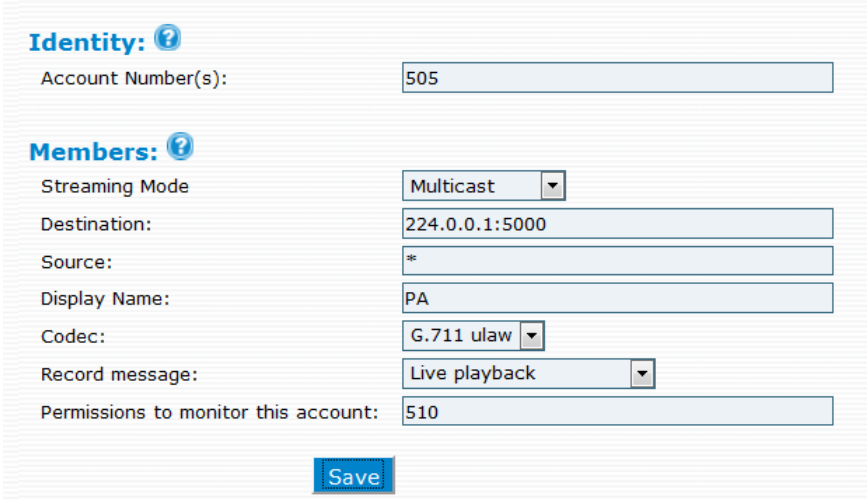
Creating a Multicast Paging Account

This section provides instructions for creating a multicast paging account on the system.

1. From the **Accounts** tab, click **Create** and select **Paging** from the dropdown.
2. Enter an account number and name, then click **Create**.


Settings
Accounts
Trunks
Dial-Plans
Status
Admin
List
Create
Create New Accounts:
Accounts are numbers that you can call on the PBX. Please select the account type that you would like t
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up sev
slash between the names, you will set up one account with different alias names. For example, "123/theo
accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
Paging
Account Names (e.g. "123/f.feuerstein"):
505
Create

3. Once the account has been created, click **List** to open the account and configure it as detailed below:



- **Streaming Mode**: From the dropdown, choose **Multicast**. Multicast mode allows you to designate an IP address as your paging group and create paging groups that encompass entire organizations. All devices that are configured to listen on the same multicast IP address will go into paging mode as soon as they receive RTP traffic on that port.

  Note: Not all phones support multicast paging. Phones that do have this support can be configured through the phone's web interface.

- **Destination**: Enter an IP address into this field. The loopback address is especially important since the paging application and the system are running on the same system.

  Note: Multicast addresses range between 224.0.0.0 and 239.255.255.255.

- **Source**: List the extensions that are allowed to page this group. Enter a star (*) to give access to all extensions.

- **Display Name**: The display name will be used to identify the source of the call. SIP phones will display this text in the display area.

- **Permissions to monitor this account**: Enter the extensions that are permitted to monitor this account.

4. Click **Save**.

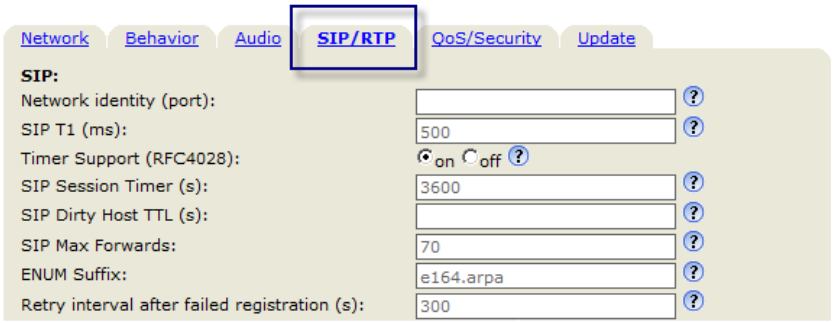
5. From any registered SIP phone, dial 75 (which is the number assigned to the paging account in this example). You should hear the audio from the speakers connected to the audio OUT on the PC. The system will send paged audio to the `127.0.0.1:5000` and the paghoh application will read from port 5000 and write to the audio OUT device.

Assigning Multicast IP Addresses to IP Phones

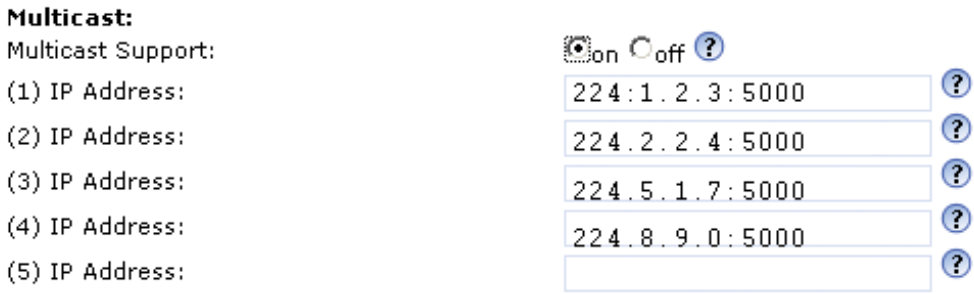
To be part of a multicast paging group, a phone must have a multicast IP address that matches the snom ONE multicast IP address. To do this, you will need to configure the multicast settings for each phone.

1. Go into the phone's web GUI by entering the phone's IP address into a web browser. The following screen will appear:

2. Click **Advanced** at the left-hand section of the screen.
3. Select **SIP/RTP** as shown below:



4. Scroll to **Multicast** at the bottom of the page.
5. Enable Multicast Support.
6. Enter the IP address that was entered as the destination when configuring the paging account (refer to page 387).



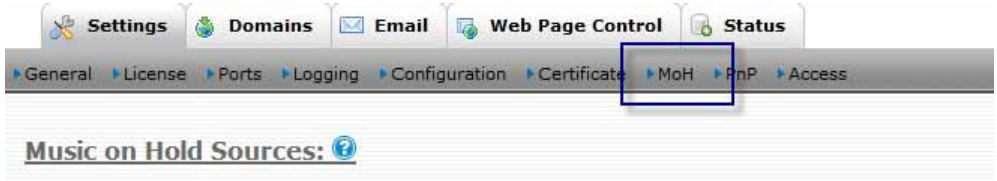
7. Click **Save**.

The phone can now pick up the RTP stream and begin playing it.

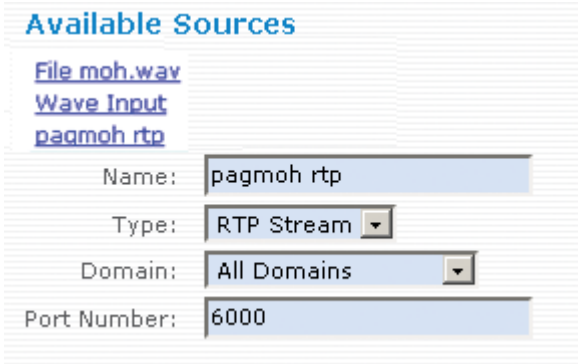
Configuring Music on Hold

This section shows you how to create the new RTP stream-based MoH source.

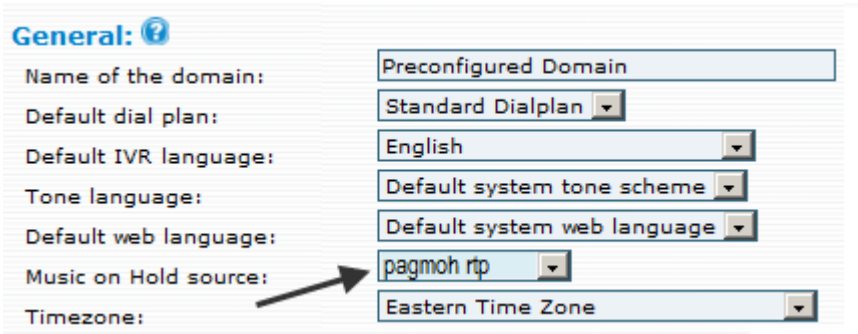
1. From the domain, click **Admin** > **Settings** > **MoH**, as shown below.



2. Use the following settings to configure the Music on Hold source:
   - **Name:** Click `pagmoh rtp` from the available sources.
   - **Type:** From the dropdown, choose **RTP Stream**.
   - **Domain:** Choose the domain(s) that will be using the Music on Hold.
   - **Port Number:** The default port is 6000.



3. Define `pagmoh rtp` as the MoH source within the domain where it will be used. Do this by going into the domain's default settings (**Domains** > **Settings**), as shown below.



4. Plug in the music source to the audio-in (generally the microphone input) of the PC that is running the pagmoh and the system. Make sure that the music is really being played on the music source.
5. Pick up a phone, make a call, and place the call on hold. From the phone that is on hold, you will hear the music from the music source.

XML Configuration File

The configuration options in the XML file are set in the *parameter*:value format. Available parameters and sample values are shown below:

Table 21-1. Available Options in **pagmoh.xml**

Parameter	Function	Example
page	Defines the port where to listen for RTP traffic. If specified, it binds the socket to the provided address.	5000
moh	Defines where to send the MoH stream. If the destination contains only the port number, the destination is the loopback device.	6000
log	Sets the log level. Valid levels are 0–9.	5
dev	Sets the audio device.	
priority	Defines whether the process should run at high priority or not.	True False
multicast	Joins a multicast address.	
ptime	Specifies the packet length in ms.	Multiples of 10
dtmf	Defines what codec to use for out-of-band DTMF.	
map	Sets the codec mapping. The argument is a list that maps the codec number to codec names.	l16, ulaw, alaw, gsm, g722, and g726
codec	Specifies the codec that should be used for sending. The parameter is the name of the codec.	ulaw
ipv4	Use only IPv4.	True
ipv6	Use only IPv6.	False

Chapter 22

CALL DETAIL RECORDS (CDRS)

A call detail record (CDR) is a file that contains information about recent system usage. A CDR can include the identities of the originator and the endpoint, the duration of each call, the direction of the call, and many other important pieces of information. CDRs can be used for measuring traffic, and they can also be exported to third-party vendors, which makes them useful for billing purposes.

A CDR can include the following information:

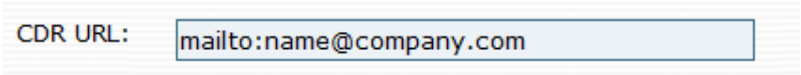
- Caller-ID
- Type of call (auto attendant, hunt group, agent group, etc.)
- CMC code
- Domain name of call
- Trunk name
- Language of call
- `From` and `To` headers
- Extension number, either originating or receiving
- Direction of call (in or out)
- Language of call
- Start time of call, as well as connected duration, answered duration, hold duration, and IVR duration
- Date and time of call
- Start and end times

CDRs for Third-Party Software Vendors

CDRs can be exported to third-party software vendors for a wide range of purposes. When used for this purpose, CDRs can be exported to the following formats:

- CSV (comma separated files)
- SOAP (XML)
- Email (sent as attachments)

To specify which format you want the system to export, you must use the **CDR URL** setting. This setting is located in **Admin** > **Settings** (see Chapter 2).



In the example shown above, the CDR will be sent to `name@company.com` once the call is finished, and the CDR will be sent as an email attachment. Other options are available when exporting CDRs. These options are shown below:

File Type	Syntax
CSV	`file:disk`
Email	`mailto:name@company.com`
Simple TCP	`cdr:<server IP:port>`
SOAP/XML	`http://`
	`https://`

CDRs that are used for this purpose automatically include the following fields:

Table 22-1. Default Fields for CDRs

Field	Values
`From`	`"00432638316014" <sip:+432638316014@company.com;user=phone>`
`To`	`"Steve Fuller" <sip:411@company.com>`
`Call-ID`	`0080-1008-25C105DA-0@D141DFC50C7AA2248`
`Direction`	`I`
`Remote`	`+432638316014`

Field	Values
Local	411
TrunkName	PSTNGateway
TrunkID	1
Domain	company.com
LocalTime	20100310105708
Start	20100310095708
Connect	20100310095710
DurationHHMMSS	0:00:10
DurationSec	10
End	20100310095720
IPAdr	udp:192.168.0.248:5060
Record_Location	Indicates the location of the file

CDR to CSV

To generate CDR files on the local disk in CSV format, use `file:disk` in the **CDR URL** setting and specify a string that will be representative of both the filename and the contents of the CDR. The default value is `$c/$m/$d` (cdr/domain/date).

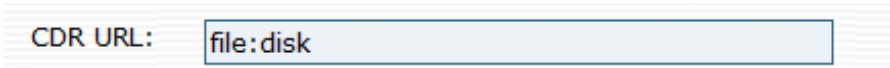


Table 22-2 shows two examples in which the CDR URL setting has been set so that CDRs will be saved as CSV files. This file represents all calls that occurred on Dec. 10, 2008. The second file represents all calls that occurred on Dec.11, 2008 between 10–11 a.m. (The $h is replaced by a number between 1 and 24.) You can configure the *cdr_file_name* setting through **HTTP** also.

Table 22-2. Setting the CDR URL Setting for CSV Output

CDR URL Setting	File Created
cdr_file_name=$c/$m/$d.csv	cdr/localhost/20081210.csv
cdr_file_name=$c/$m/$d/$h.csv	cdr/localhost/20081211/10.csv

Notes:

It is advisable to always use `$c` as the first variable.

Each CDR line will be terminated with `\r\n`.

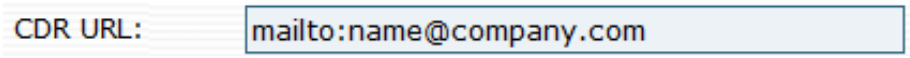
The default field separator for CSV files is a comma (,). You can change this by using the *`cdr_field_separator`* global setting.

If you want to save the CDRs to a mapped drive, configure the *`cdr_file_name`* setting to `z:/cdrs/$d.txt`.

Example: `http://<snomone address>/reg_status.htm?save=save&cdr_file_name=z:/cdrs/$d.txt`, where `<snomone address>` is your system's address.

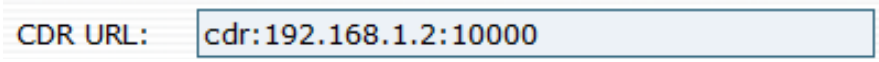
CDR to Email

To send CDRs to a third party as email attachments, use `mailto` in the **CDR URL** setting, and specify an email address:



CDR to Simple TCP

Several commercial tools are available for collecting CDR information through simple TCP-based communication. Each CDR is sent in one line of ASCII text terminated by a CRLF pair over a TCP-based communication link. To differentiate the destination from a SOAP CDR, use `cdr` in the **CDR URL** setting in front of the IP address and the port (the fields are separated by a colon).



If you want to change the default settings of CDRs on the system, you can modify *`cdr_format`* in the global configuration file. This file is located in the working directory of the system and is named `pbx.xml` by default. It is a standard XML file, is encoded in UTF-8, and contains configuration information which cannot be assigned to any specific domain. Before making changes to the file, be sure to make a backup. And once changes have been made, restart the service.

When customizing the *cdr_format* string, you can use the fields shown in Table 21-3. Both the short form and the long form of all fields are included. You can use either format or switch between the two formats. When specifying lengths, put the length of the string between the dollar sign and the character. For example, the expression `$10c` will insert a 10-digit caller-ID into the string. Following is a sample string that specifies lengths. The resulting output is also shown:

Sample String	Sample Output
`$w$5e$12c$5d`	`20071023123024 123 9781234567 120`

Table 22-3. CDR Formats—Short and Long

CDR Syntax		Description	Value
Short	Long		
`$$`	`$$`	A dollar sign	`$`
`$i`	`$(call_id)`	Caller-ID of call, as seen in the SIP packet	
`$v`	`$(call_type)`	Type of call. Default is `attendant`*	`attendant`
`$m`	`$(domain)`	Domain name of the call	`domain.com`
`$l`	`$(lang)`	Language of the call	`en`
`$f`	`$(sip_from)`	The `From` header, as seen in SIP packet	
`$t`	`$(sip_to)`	The `To` header, as seen in the SIP packet	
`$F`	`$(calling)`	Extension number of the caller	`123`
`$T`	`$(called)`	Extension number of the called party	`123`
`$x`	`$(orig_trunk)`	Name of originating trunk, if present	`Trunk 1`
`$y`	`$(dest_trunk)`	Name of destination trunk, if present	`Trunk 1`
`$R`	`$(account)`	Account that is charged for redirected call	

CDR Syntax		Description	Value
Short	Long		
$r	$(redirect_dest)	Destination for a redirected call (used only if call is redirected)	
$S	$(start_time)	Start time in seconds	
$C	$(talk_duration)	Connected duration of the call	
$A	$(ring_duration)	Answered duration of call (useful if the call is ringing/answered through queue)	
$E	$(hold_duration)	Hold duration for the call	
$W	$(wait_duration)	IVR duration for the call	
$w	$(start_date_time)	Start time (YYYYMMDDHHMMSS)	20071023123224
$b	$(date)	Date (YYYYMMDD) (version 2.1.9)	20071023
$B	$(time)	Time (HHMMSS) (version 2.1.9)	
$e	$(extension)	Extension number of call (originating or receiving)	
$o	$(direction)	Direction of call (i for inbound; o for out)	i or o
$c	$(remote_call_id)	Caller-ID of remote party	
$d	$(duration)	Duration of call in seconds (inc. hold time)	
$s	$(extn_duration)	Speaking duration (does not inc. hold time)	
$M	$(cmc)	Client matter code (CMC)	781299
$(record_location)		The location of recorded files	

* Other values include attendant, acd, ivrnode, hunt, conference, mailbox, extcall, starcode, and srvflag.

Note: The dollar sign has a special meaning. If you would like to produce an actual dollar sign, use two dollar signs ($$) as the value.

Sample Strings

Following are sample strings that can be used to change the CDR format:

- *Example 1*: `cdr_format=$w$m$F$T$o$d$R,$c$v$(record_location)$e,$(cmc)`
- *Example 2:* `cdr_format=StartTime:$w,Domain:$m,From:$F,To:$T,Dir:$o,RemoteCID:$c,Type:$v,Rec:$(record_location),Extn:$e`
- *Example 3:* `cdr_format=$16w$10m$32F$32T$2o$16d$10R$16c$v$(record_location)$4e`

  Although example 1 (the short form) is more concise, example 2 (the long form) is easier to decipher. The third example reflects specified lengths.

Making Changes through HTTP

If you'd prefer not to make changes to the global configuration file, you can use the web interface to create a request that will change the *cdr_format* setting. For example, if you want to change the CDR format of a system running on a localhost, you would enter something like this (replace `localhost` with your snom ONE address):

```
http://localhost/reg_status.htm?save=save&cdr_format=$w$5d$
25m$2o$20F$20T$20R$20r$15c$20f$15v
```

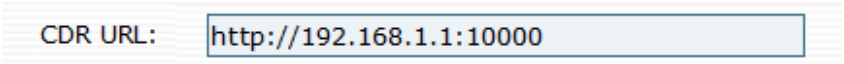
You can also use the web interface to make changes to the *cdr_file_name* setting:

```
http://localhost/reg_status.htm?save=save&cdr_file_name=
$c/$m/$d.csv
```

CDR to SOAP/XML

The CDR SOAP mechanism can communicate with an external web server. The system starts a SOAP call to a URL specified in the system each time a call is completed. The third-party web script which receives the SOAP call will then parse the XML packet and file the data in the required place. The storage of the data is outside of the system and is the responsibility of the integration team.

To send CDRs to an external SOAP server, use `http://` or `https://` in the **CDR URL** setting and specify the IP address and port number:



snom ONE

Part III
The User Interface

Chapter 22

WEB INTERFACE

The web interface is one of the most important differences when comparing modern-day VoIP systems with legacy IP-based systems. The web interface allows users to integrate their cell phone and configure other settings related to their account. Before users can access the web interface, they will need the URL of the system and a user name and password. This information can be sent to users at the time the extension is created in the form of a welcome message (other methods can also be used). The **Send welcome email** setting is a domain administrator setting and is mentioned on page 95.

Logging in

When users log in, the default of **Automatic** can be used for the login type; however, if a user has been given administrator or domain administrator privileges and wants to log in as a user for any reason, **User Login** must be selected from the dropdown (see Chapter 1 for more information on logging in).

Figure 22-1. Web Interface Login Screen

Once the user has logged in, the web interface shown in Figure 22-2 will be displayed.

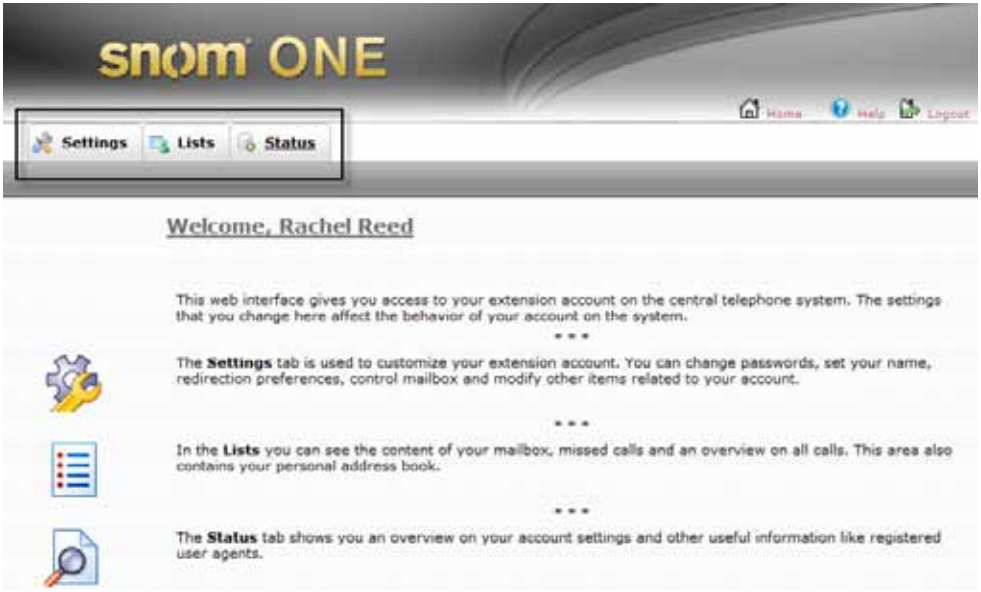

snom ONE
Settings
Lists
Status
Welcome, Rachel Reed
This web interface gives you access to your extension account on the central telephone system. The settings that you change here affect the behavior of your account on the system.
The Settings tab is used to customize your extension account. You can change passwords, set your name, redirection preferences, control mailbox and modify other items related to your account.
In the Lists you can see the content of your mailbox, missed calls and an overview on all calls. This area also contains your personal address book.
The Status tab shows you an overview on your account settings and other useful information like registered user agents.

Figure 22-2. Web Interface Welcome Page

These tabs are detailed below:

- The **Settings** tab allows users to change their password, set up redirection, and control their mailbox. Voicemail, buttons, and instant message settings are also located here.
- The **Lists** tab allows users to access important lists: email, missed calls, and personal and domain address book contacts. Also from the **Lists** tab, users can schedule conferences.
- The **Status** tab displays a snapshot of the user's account settings. Users can quickly see their call forwarding, hot desking, and agent status.

The following pages cover the settings that users can make from their own accounts. Other settings that are not shown here can also be configured from the user's account (permission and registration settings). These settings are visible only to administrators who log into the user's account (these settings are detailed beginning on page 167).

Extension Settings

This section describes all the configurations that can be made from the **Settings** tab:

Once the user clicks the **Settings** tab, the web interface will present the following new options to the user:

- **General**: This is where users can change their password, upload their picture, and specify pickup preferences.
- **Redirection**: From this link, users can activate "Do not disturb," establish treatment for anonymous callers, and set call forwarding. Cell phone configuration can also be done here.
- **Mailbox**: Users can enable their mailbox, set a pickup time, assign a maximum number of messages that can be sent to their mailbox.
- **Email**: Users can add an email address to their account and establish email account settings.
- **Buttons**: This is where users can configure a button profile.
- **Instant-Message**: From this link, users can send instant messages from the web interface.

General Settings

From the **Settings** tab, the settings shown in Figure 22-3 will be displayed. Administrators can block some of these settings to prevent the user from changing them (see Figure 2-4 on page 78 for more information).

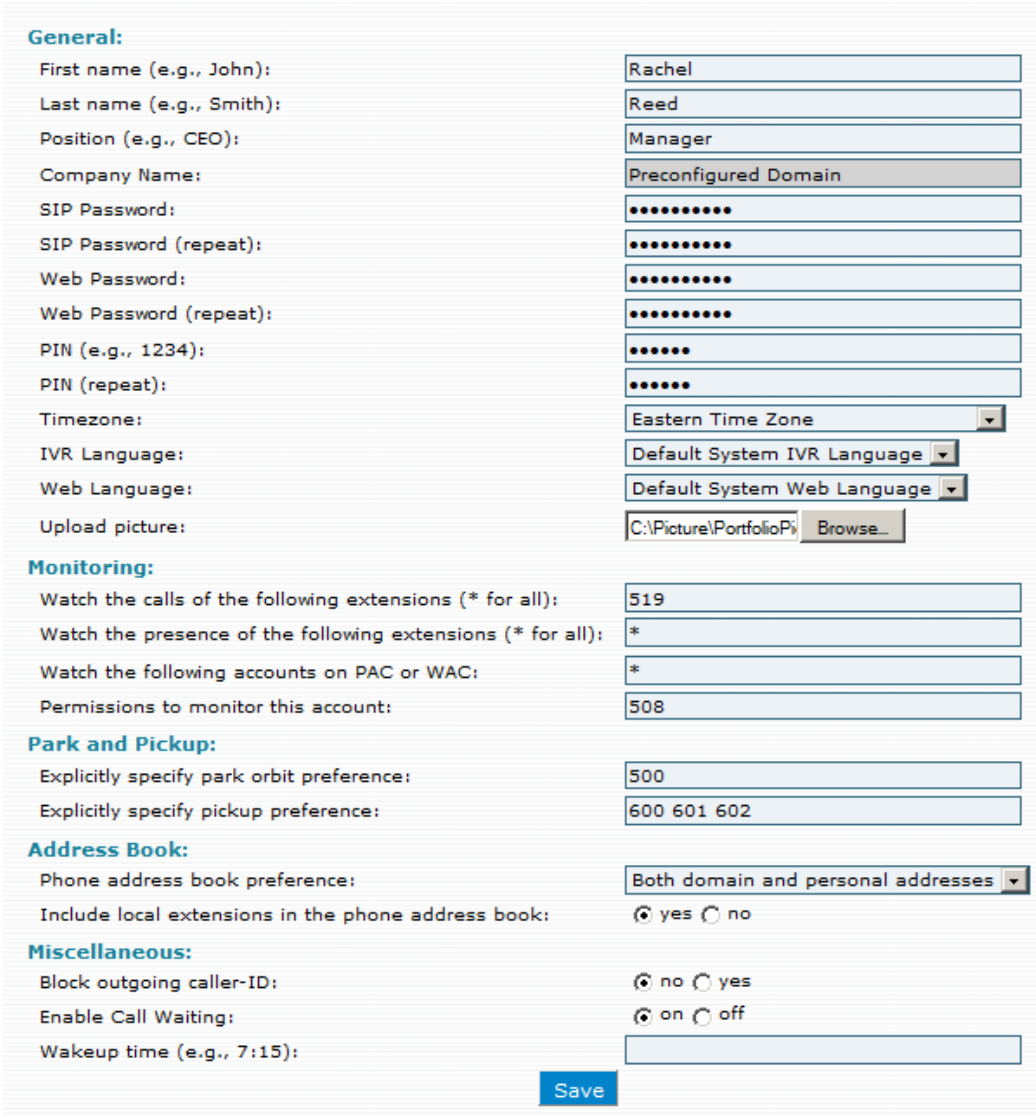


Figure 22-3. User's Settings Tab

The settings shown in Figure 22-3 are detailed below:

General

- **First name and Last name**: These fields will be displayed for all internal and external calls (international characters are permitted).
- **Position:** This field is for the user's position/job function in the company.
- **Company name:** This field is reserved for the company name.
- **SIP Password**: The SIP password influences the connection between the VoIP phone and the system. Users should not change this password, as it will interfere with access to other registered SIP devices (e.g., soft phone).
- **Web Password**: This password is used to access the snom ONE web interface.

  Note: Use a combination of letters and digits and even a symbol to ensure password security. After you've entered a new password, the current HTTP session will stay valid until your next login. Permanent cookies will be invalidated on the next login.
- **PIN**: The user's PIN will be used in several areas of the system (e.g., when accessing their voicemail from an outside phone, when using the calling card account, and when hot desking). For optimum security, user's should be required to use at least five digits.
- **Timezone**: This setting tells the system the user's time zone. It will affect the time stamps of the mailbox and all other time stamps related to the extension. When using the extension from a time zone that differs from the domain's time zone, users will need to override the domain setting.
- **IVR Language**: This setting controls the language of voice prompts delivered by the system, as well as the language that is displayed on the LCD of the user's phone. (Callers will not hear the language when calling into the user's mailbox.) Administrators can add additional languages onto the system (see page 321 for instructions).
- **Web Language**: This setting allows users to control the language of the snom ONE web interface and in the emails they receive from the system. Users can override this setting during their initial login to the web interface.

- **Upload picture**: The uploaded picture will be displayed whenever the user calls another extension within the same domain (as long as the other extension has picture-displaying capability). To facilitate easier picture upload during the call setup, users should use a thumbnail image size. The format of the picture depends on phone model:
  - For snom 370 phones: Grayscale BMP image.
  - For models that can display color photos: JPEG image.

    The system will display the picture on the landing page of the snom ONE web interface.

Monitoring

- **Watch the calls of the following extensions**: This feature allows users to watch the presence of an extension(s). The system will automatically generate configuration files of the extensions specified.

  Note: Wildcard patterns are permitted in this field. If only a star is used, the system will place all extensions of the domain into its call-watching list.
- **Watch the presence of the following extensions (* for all):** This setting is similar to the previous setting, but it doesn't provision calls. Instead, it asks the device to subscribe to the presence state of the listed extensions. The system will forward the presence state of the phones, but the phones themselves will be responsible for generating the presence information.
- **Watch the following accounts on PAC or WAC**: This setting allows users to list the extensions they would like to monitor from the WAC. When using the WAC, this setting enables users to join a conference room (the conference room must be included as one of the extensions that will be monitored).
- **Permissions to monitor the account**: This setting allows users to specify the extensions that are permitted to see the status of their extension, including their active calls. By default, all extensions are allowed to see the status of other extensions. A user can either list the extensions (e.g., 511, 518, 523, 522, 513) or use wildcards to match multiple extensions (e.g., 5*).

Park and Pickup

- **Explicitly specify park orbit preference**: This setting allows users to specify a list of park orbits that can be used for parking calls. When park orbits have been entered into this field and the user executes the Call Park (*85) feature, the system chooses the first available orbit. When a star (*) is entered into this field, the system will have no preference list to draw from, and the user will be required to enter the number of the park orbit after entering *85 (see page 434 for more information on Call Park).
- **Explicitly specify pickup preference**: This setting allows users to specify the accounts that will be picked up when they execute the Call Pickup (*87) feature. This setting is especially useful when extensions have been grouped with certain agent groups and hunt groups, as it will prevent the wrong calls from being picked up. If a star (*) is entered into this field, the system will have no preference list to draw from and will require a park orbit number after the *87 (see page 435 for more information on Call Pickup).

Address Book

- **Phone address book preference**: This setting allows users to upload contacts from the domain and personal address books to their phones. Available options are as follows:
  - Both domain and personal addresses
  - Domain addresses only
  - Personal addresses only
- **Include local extensions in the phone address book**: This setting allows users to add extension numbers from the system to their phone.

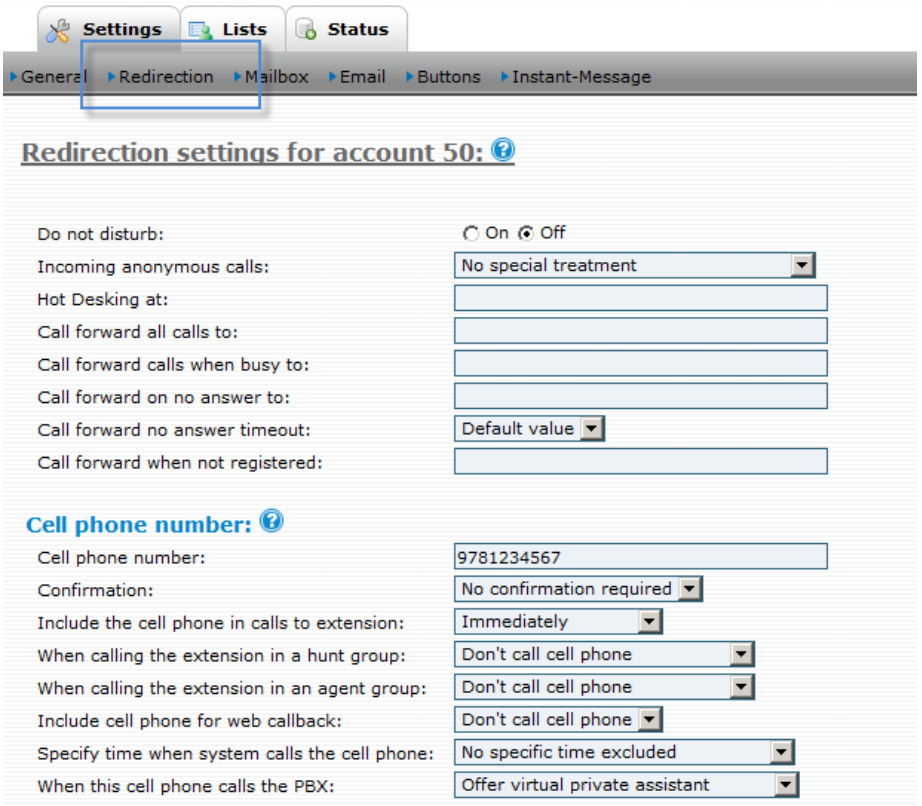
Miscellaneous

- **Block outgoing caller-ID**: This setting allows the user to control whether their caller-ID is shown when making outbound calls.
- **Enable Call Waiting**: This setting allows the user to turn Call Waiting on and off.

- **Wakeup time**: This field allows users to receive automatic wakeup calls from the system. Though this feature is used primarily in hospitality environments, it can also be used on an individual basis. A wakeup call can also be activated using star code *62. See “Wakeup Call (*62)” on page 447.

Redirection Settings

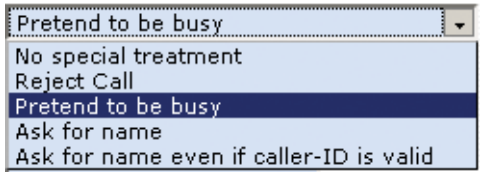
Redirection settings allow users to forward their calls to other extensions or phone numbers. These settings are detailed below (cell phone redirection settings are detailed in Chapter 25):



- **Do not disturb**: This setting allows users to tell the system to leave their phone silent for all calls, both internal and external, and even calls from the hunt group. Only extensions with permission to override DND will be able to call the extension. DND override is an administrator setting (see **Call the**

following extensions even if DND is set on page 174). An extension on DND can place outbound calls at all times. You can also set DND using the star code. See "Do Not Disturb (*78)" on page 443.

- **Incoming anonymous calls**: This setting controls the treatment of incoming calls; however, it does not affect internal calls or calls from a hunt group or agent group. See also the Black List (*92) feature on page 449.



  - **No special treatment**: All calls are sent directly to the user's extension.
  - **Reject Call**: The caller will be informed that the user does not accept anonymous calls and will not be put through to the extension.
  - **Pretend to be busy**: This setting prevents the call from going through but does not tell the caller why.
  - **Ask for name**: The caller is prompted for his or her name and then put on hold while the extension is called. After the system reads out the recorded name, the user can decide whether to accept the call, send it to the mailbox, or reject it.
  - **Ask for name even if the caller-ID is present**: This setting requests the caller's name, even if the caller-ID is available. Only white list callers will be put directly through.

- **Hot Desking at**: This setting allows users to specify an extension where they will pick up their calls. All calls (including calls from an agent group or hunt group) will be sent to this extension. For more information on hot desking, see page 439.
- **Call forward all calls to**: This setting allows users to redirect all calls to another extension. Only calls that are headed directly to the user's extension will be affected by this setting. If a user is part of a hunt group, agent group, or paging group, calls originating from these groups will not be redirected.

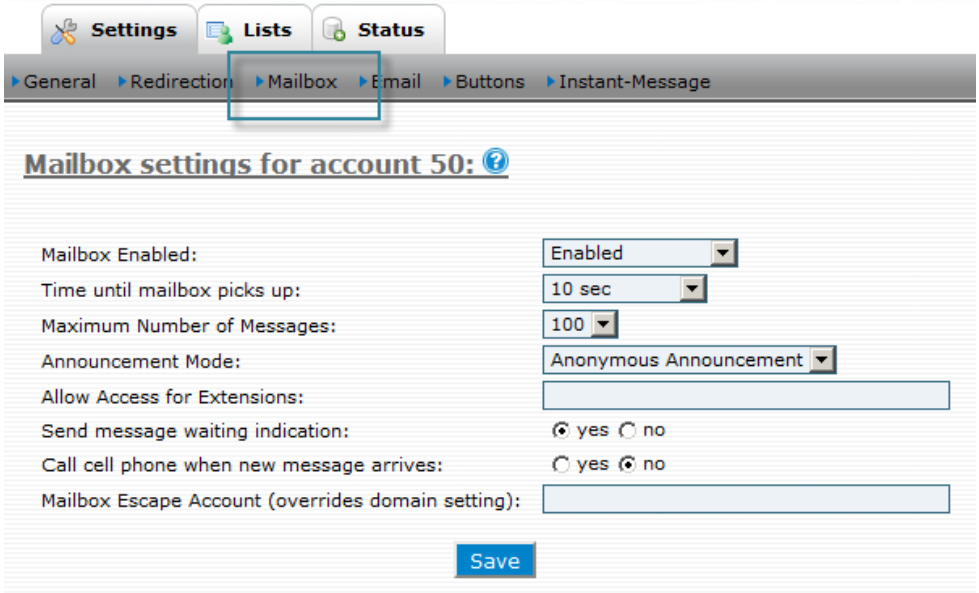
- **Call forward calls when busy to**: This setting allows users to forward all calls to the extension that is specified, only when the extension is busy. This condition is true if either the phone itself signals that it is busy or if the lines parameter (page 170) has been set for the extension and this number has been reached.
- **Call forward on no answer to**: This setting allows users to redirect all calls after there has been no answer for a predefined period. The waiting period is defined in the domain but can be overridden by the **Call forward no answer timeout** setting (next bullet item). (If the mailbox picks up earlier, this setting will have no effect; if the call is redirected, the mailbox timeout will be cancelled.)
- **Call forward no answer timeout**: This setting determines how long the system will wait for the user to answer the phone before forwarding the call (default is 10 seconds). This field is effective only if the **Call forward on no answer** field has been set.
- **Call forward when not registered**: This setting allows the user to specify where calls will be forwarded if the user's extension is no longer registered for any reason. If the user is part of a hunt group, agent group, or paging group, calls originating from these groups will not be redirected.

Cell phone settings are discussed in Chapter 25 beginning on page 467.

Mailbox Settings

Every extension has a voice mailbox on snom ONE; however, the administrator can disable users' mailboxes and use an external mailbox, such as Microsoft Exchange. This section applies only to the voice mailbox of the system. Mailbox settings are located in **Settings** > **Mailbox** and are detailed below:

- **Mailbox Enabled**: From this setting, users can enable or disable their voice mailbox. If it is disabled, callers will not be able to leave messages and the user will be unable to use the mailbox functions. If **Act as park orbit** is chosen, those who call the extension will be parked at the extension until their call is picked up. This is obviously not useful for extensions that have phones registered and make phone calls.



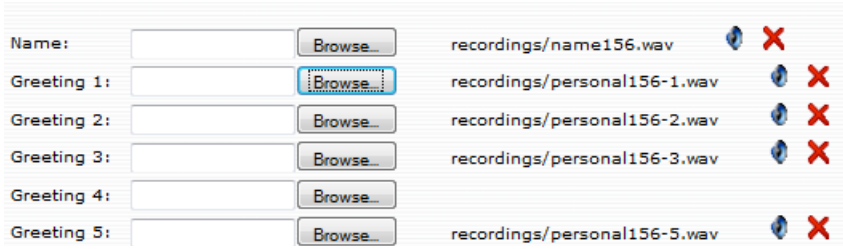
- **Time until mailbox picks up**: This setting allows users to specify how long the system should wait before redirecting calls to the user's voicemail. If **Call forward no answer timeout** has been set (see Redirection settings on page 410), the shorter timeout will be executed first. If **Include the cell phone in calls to extension** has been set (see Redirection settings), the system must be given enough time to call the user's cell phone (which may take 10 or more seconds) and enough time for the user to view the caller-ID. The default is 20 seconds.
- **Maximum number of messages**: This setting allows the user to specify the maximum number of voicemail messages that should be stored at any one time. If the maximum has been reached and a caller wants to leave a new voicemail message, the system will attempt to delete a saved message. If space is still unavailable, the system will inform the caller that the mailbox is full.
- **Announcement Mode**: From this setting, users can choose an announcement that callers will hear when reaching the their extension.
  - Anonymous Announcement: The caller will hear the number of the extension.

  - Name Announcement: The caller will hear the recorded name of the extension, if one is available.
  - Personal Announcement: The caller will hear the recorded announcement of the extension, if one is available.

- **Allow Access for Extensions**: This setting allows users to create a group mailbox. A group mailbox can be used for anything from a joint boss/secretary mailbox to a place to collect after-hours calls or holiday calls. All parties will be notified of incoming messages by the MWI that is located on *their individual phone* (see MWI below). Users can listen to the messages from either their own voice mailbox or by dialing into the shared mailbox from an outside phone or an outside line on their own phone (see page 454 for instructions on accessing voicemail from an outside phone). Dialing *directly* into the shared mailbox allows users to hear messages that were called into the shared extension only (i.e., the messages will not be mixed with the user's own voicemail messages). Users will need the PIN of the shared mailbox when accessing it directly.

  When entering multiple extensions into this field, use a space as a separator (e.g., `101 102`).
- **Send message waiting indication**: When this feature is activated, users will receive a message waiting indicator (MWI)—a blinking light on their phone—that notifies them of a new message. Once the user has listened to the message, a solid light will replace the blinking light. This enables the system to alert the user the next time a new message has arrived. Star code *99 will clear the message indicator even if messages have not been read.
- **Call cell phone when new message arrives**: If users have decided against forwarding their calls to their cell phone but still want to be alerted when a new message arrives on their extension, they can activate this feature. Once a caller has left a message, the system will call the user on the cell phone. After the announcement, the user must press 1 to hear the message.
- **Mailbox Escape Account (overrides domain setting)**: This setting gives users the option of changing the direction that a call will take once the caller presses 0 to speak with the operator. The extension that is entered into this field will receive the calls that the user thinks are directed to the operator.

The following section of the **Mailbox** page is visible only to the administrator. From here, greetings for the user's extension can be uploaded by the administrator.



Email Settings

The email settings on this page allow users to receive emails as notification of all incoming calls on their extension. Users can also request an audio file, or WAV file, of voicemail that has been left on their extension. Email settings are located in **Settings > Email**, and the descriptions of the settings are listed after Figure 22-4.

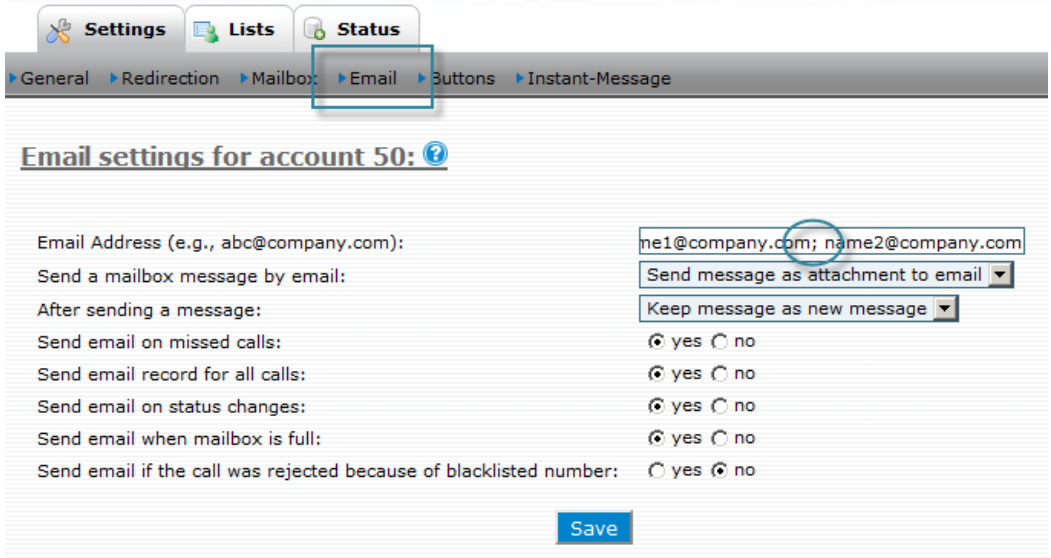
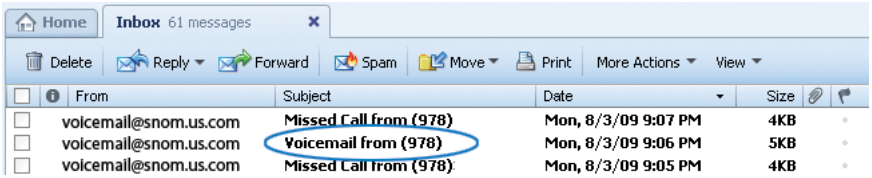


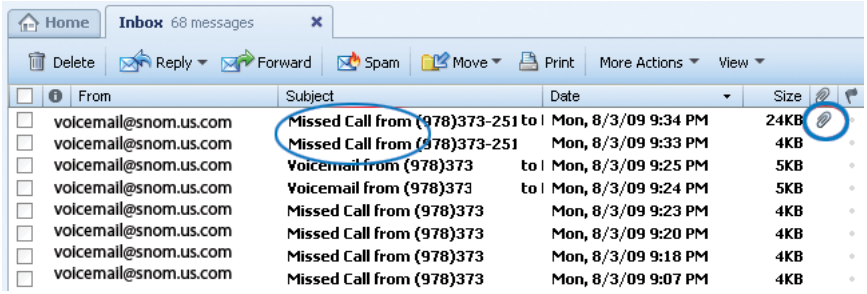
Figure 22-4. User's Email Settings

The following information details the settings that can be set from the user's **Email** link:

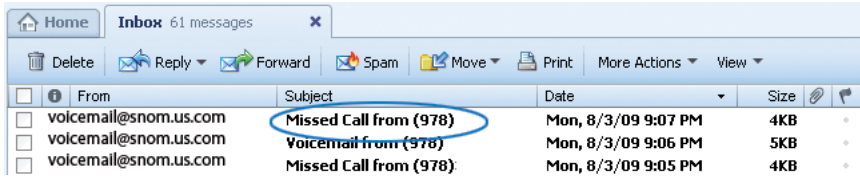
- **Email Address (e.g. abc@company.com)**: This feature allows users to integrate their email account with their extension account. Voicemail messages will be sent to the user's email account according to the settings chosen below (a semicolon is required when entering multiple email addresses into this field).
- **Send a mailbox message by email**:
  - **Do not send an email**: No email will be sent. This option should be used when the user prefers to use only the phone to receive voicemail messages.
  - **Send emails without attachments**: Email notifications will be sent to the user for every voicemail that is received. This provides somewhat of a visual voice mailbox. The user will see the name and number of the caller and the date and time that the call arrived. To retrieve the voicemail itself, the user will need to call into the voicemail. The benefit of this mode is that emails that are relatively short can easily be read using mobile devices that support reading emails.



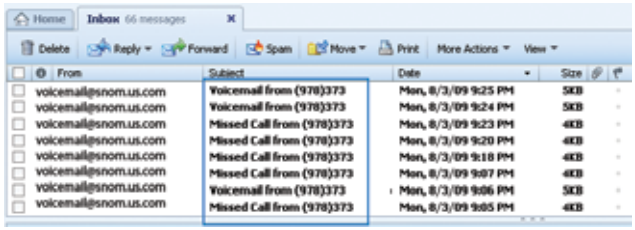
  - **Send message as attachment:** The user's actual voicemails will be attached to the email notifications. This option should be selected if email is being used throughout the day and a personal computer is being used to process the email.



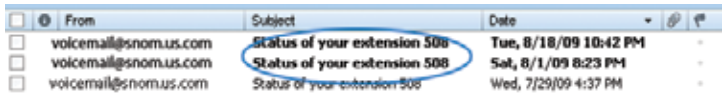
- **After sending a message**: This setting allows users to decide what to do with a voicemail message after it has been emailed to them:
  - **Keep message as new message**: The message will remain in the user's mailbox as a new message. This option has the potential danger of eventually overfilling the voice mailbox. Administrators can use the **Voicemail Size** setting (page 98) to restrict the number of voicemail messages.
  - **Mark message as read**: The message will remain in the user's mailbox, but the system will drop the oldest message to make room for new messages if the mailbox becomes full. The disadvantage of this mode is that the message waiting indicator will not alert the user of new messages.
  - **Delete the message**: The message will be deleted after the email has been sent. This keeps the mailbox clean, but because the system does not store voicemail messages permanently, the user will need to listen to the messages from the email client.
- **Send email on missed calls**: When this setting has been activated, the system sends the user an email for each missed call. Calls to a hunt group or agent group are not included.



- **Send email record for all calls**: When this setting is activated, the system sends the user an email for all calls. This feature is useful for keeping track of a group sales extension, a telemarketing campaign, or calls made to a new employee's extension. (When both "missed calls" and "all calls" have been activated, the user will receive two emails for each missed call.)

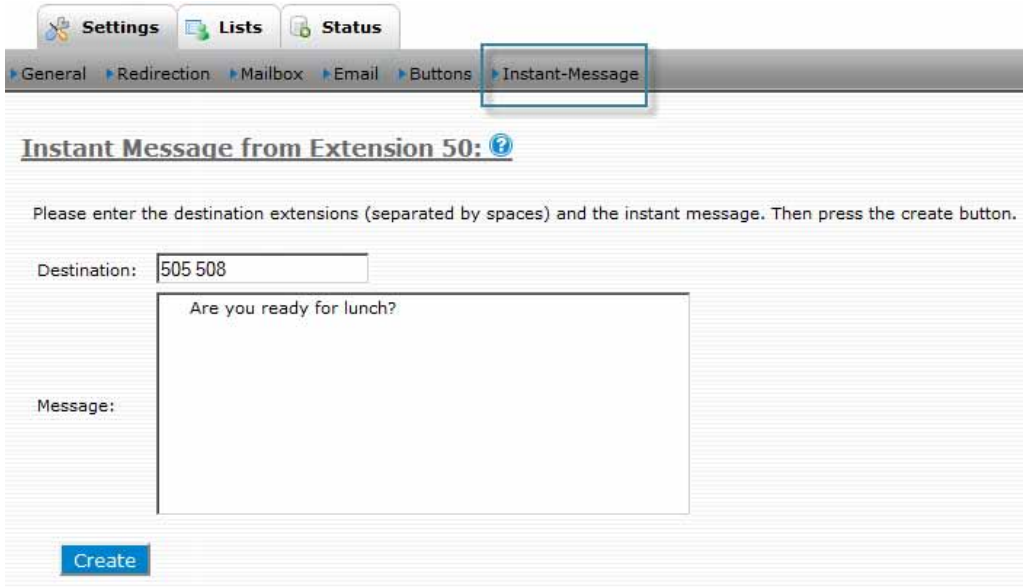


- **Send email on status changes**: The user will be notified of all status changes (e.g., toggling the DND status, changing the registration status, etc.).



Instant Message

The Instant Message feature allows users to display an instant message (IM) on the screen of snom phones. Although snom phones cannot generate IMs, they can display them. This feature comes in handy when users need to pass information along to someone during a conference call, for example. This feature is located in **Settings > Instant-Message**:



1. Enter the extension numbers into the **Destination** field.
2. Enter your message into the **Message** field.
3. Click **Create**.
4. *Note*: When multiple destinations are used, a space should be used as a separator (e.g., `102 103 208`). The system will send the message to all registered devices for the extensions that have been entered.

Call Lists

This section covers material that is related to call lists only.

Mailbox

The **Mailbox** link allows users to check their voicemail from the web interface. Call details (e.g., the caller, time of call, and length of message) are included. The voicemail list can be accessed by going to **Lists** > **Mailbox**.

- **Time**: The time the message was recorded (receiver's time zone).
- **Number**: The caller-ID and name of the person who left the message, if available.
- **Duration**: Length of message (in `minutes:seconds` format).
- **Flags**: The message can be flagged with the following icons:

	Message delete		Message marked private
	Message unread		Message marked urgent
	Download message		

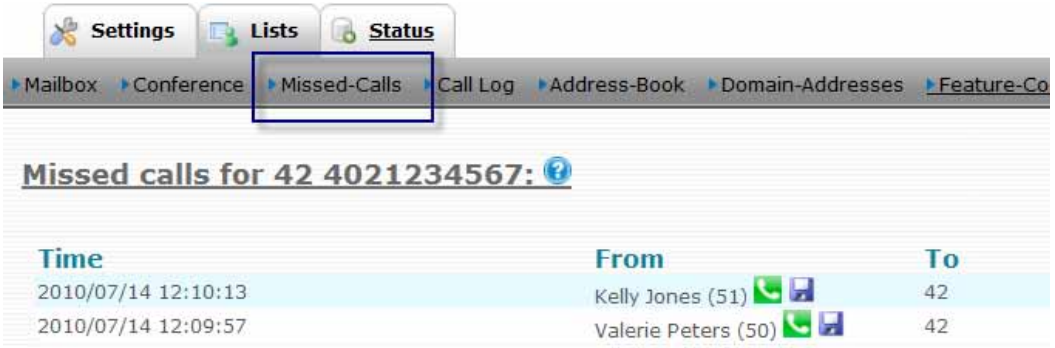
Missed Calls

The Missed Calls list allows users to view calls that were attempted to their extension but did not connect. If display names are available, the system will display them here. The length of the list is set by the administrator from **CDR listing size** (page 46). By

default, the system keeps call list records for 7 days; however, this setting can be customized by the administrator (see **Keep CDR Duration** on page 46).

The Missed Calls list displays the following information:

- The time when the call was started.
- The caller-ID and the name of the person who called
- The extension number the caller was trying to reach.



The following icons are associated with the **Missed Calls** page:

One-click dialing: Click to initiate a callback to the party who called you. The call will be charged to the user's extension.

Address book: Click to save the contact in the personal address book.

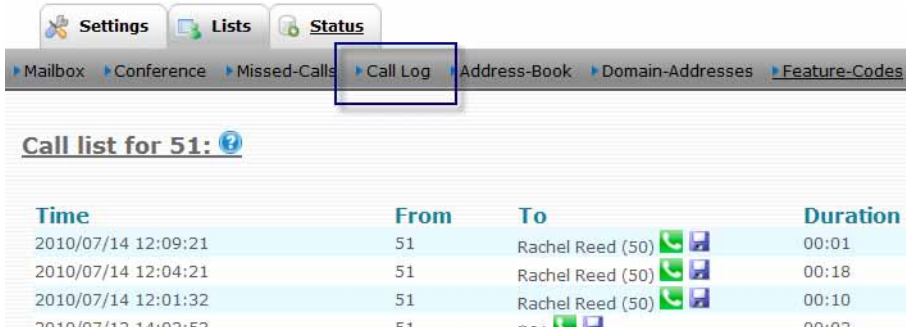
Call Log

The Call Log allows users to access up-to-the-second information for calls made to and from their extension. Each entry in the call log contains the following information:

- Time the call was started.
- Number the call was made from (display names are included when available).
- Number the call was made to (display names are included when available).
- Call duration (in minutes and seconds). If the call was not connected, the duration will be empty.

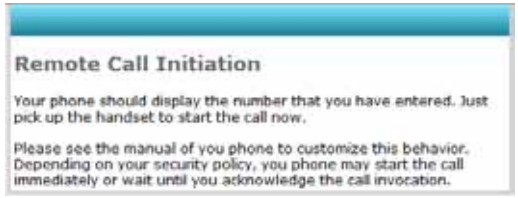
Notes:

The Call Log displays records of calls beginning with the oldest. The number of records that can be stored in the Call Log is limited by the number of lines that can fit on a user's computer screen.



From the Missed Calls page, icons are available that allows the user to initiate a callback to the party who called and to save a caller's information to the personal address book.

Click-to-dial: Allows the user to initiate a call to the calling party. When the following dialog screen is displayed, the user needs to answer the phone. The system will call the requested extension or phone number. (The call will be charged to the user's extension.)


Remote Call Initiation
Your phone should display the number that you have entered. Just pick up the handset to start the call now.
Please see the manual of you phone to customize this behavior. Depending on your security policy, you phone may start the call immediately or wait until you acknowledge the call invocation.

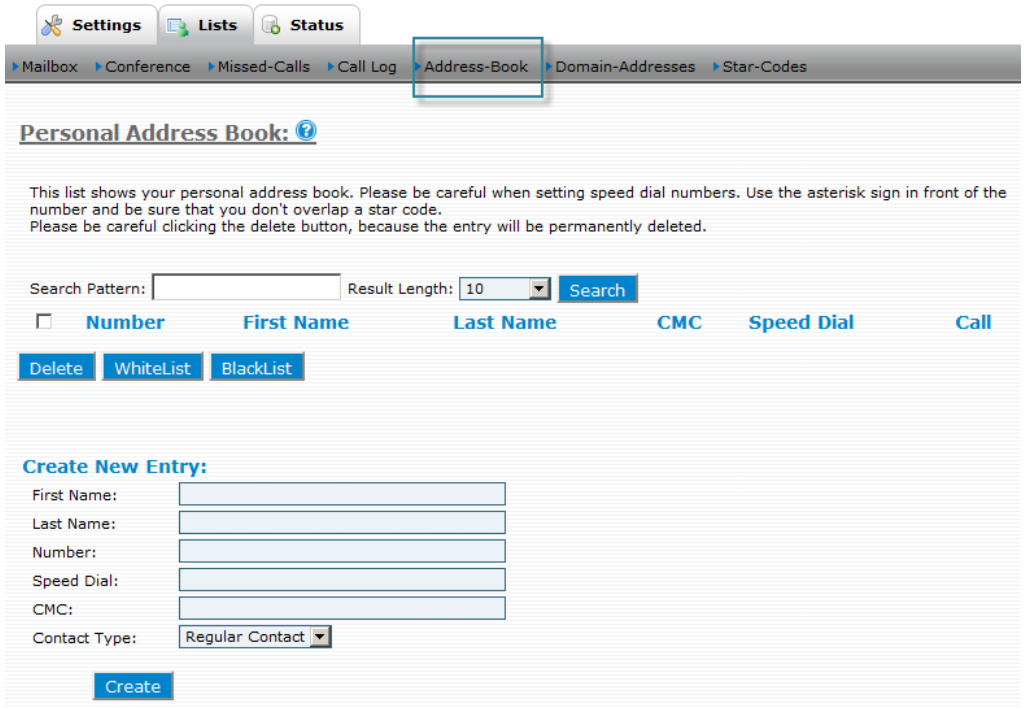
Address book: Allows users to add contacts to the personal address book:

Contacts

Address books allow users to see who's calling. They can also be used to expedite billing (when a CMC is used) and to speed-dial contacts. The system offers two types of address books: a personal address book, which is private for the extension, and a domain address book. The latter is visible to the entire domain but is not editable by its users. This section covers both the personal and the domain address book.

Personal Address Book

Users can access the personal address book by logging into the web interface and going to **Lists** > **Address Book** as shown below:



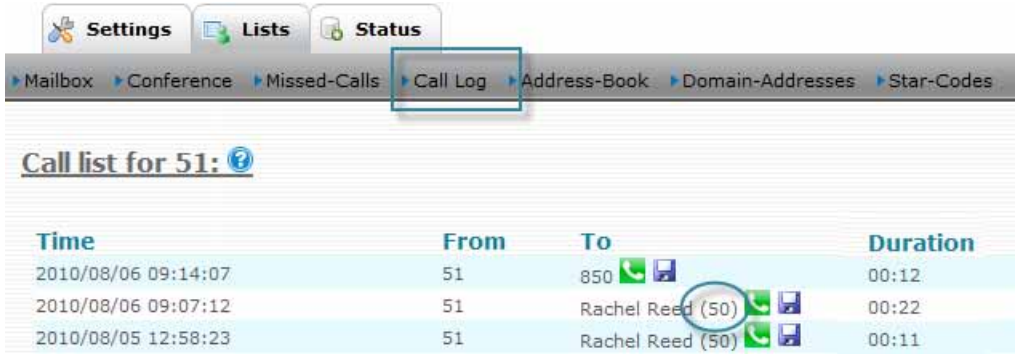
From this page, users can edit and delete existing address book entries and create new entries.

Create Address Book Entries

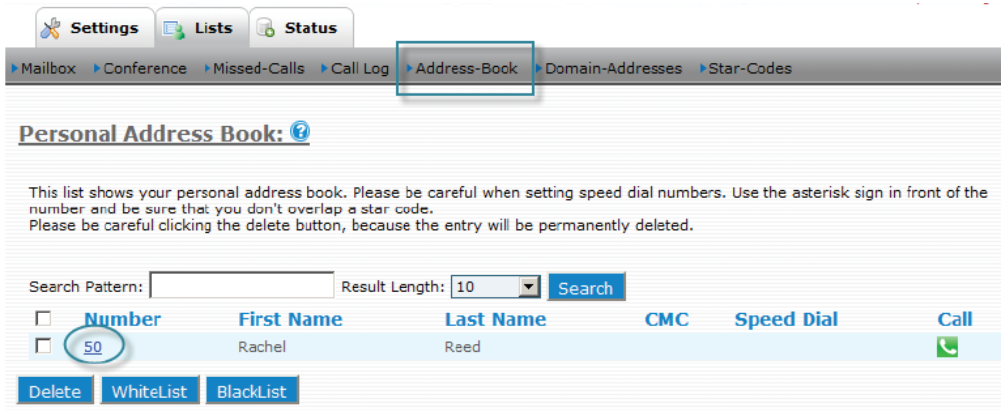
Users can add a contact to their personal address book using two different methods.

Method 1—Using the Call Log: If the contact is in the user's Call Log (i.e., contact has been made by either the user or the caller), the following instructions apply:

1. Click **Call Log** from the **Lists** tab (shown below).
2. Click the Address Book icon.



The contact will be added to the user's address book:



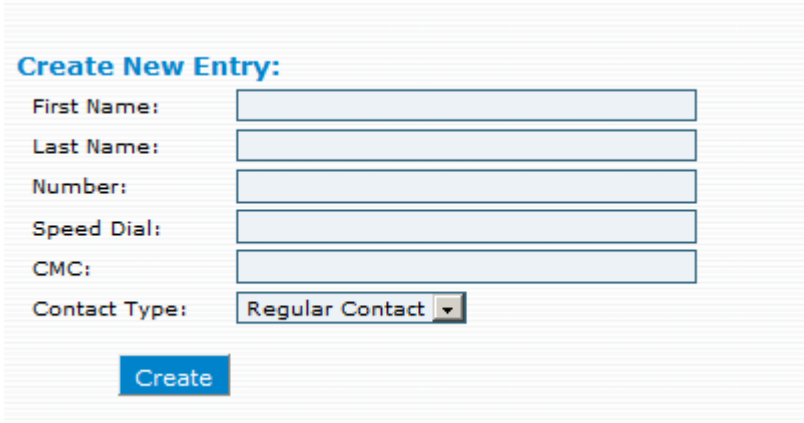
3. If you add a contact whose information is incomplete, click the account number and populate the necessary fields:

- **First Name**: Enter the first name of the contact if one was not available.
- **Last Name**: Enter the last name of the contact if one was not available.
- **Number**: Enter the telephone number of the contact (this is not a SIP URL). (This field will already be populated if this contact was in your Call Log.)
- **Speed Dial**: Enter a 2-digit star code (e.g., *12) to speed-dial this contact.

  Note: Ensure that the star code does not overlap with any of the standard star codes.
- **CMC**: The client matter code identifies the customer and is used to expedite billing in offices that bill their clients for phone calls (e.g., a lawyer's office).
- **Contact Type**: Using the dropdown list, identify the contact type.
  - Regular Contact
  - White List: The white list usually contains contacts that are trusted. If the flag is set to White List, the contact becomes part of the white list and gets preferred treatment. Contacts on the white list are never intercepted by the auto attendant and will not need to state their name. Callers on the white list are allowed to receive a callback when the extension becomes available.
  - Black List: The black list usually contains the list of contacts that users would prefer to avoid. If a caller is on the black list, the user's anonymous call treatment settings will determine how that call is treated (see **Redirection**). If the caller should be blocked, then the system will block that call. Otherwise, the system will ask the person to leave his name before calling your extension. Black list contacts are not allowed to camp on an extension.

4. Enter comments that are relevant to the contact.
5. Click **Create**.

Method 2—Using the Address Book: If the contact is not in the user's Call Log, users can add entries to their address book by going to **Lists** > **Address Book** and populating the following form using Steps 3 through 5 above:



Note: Contacts can also be added to the address book by using the black list (*91) and white list (*92) star codes. If the number does not exist, the system will automatically create an address book entry for the number. Users can edit the entry by going to **Lists** > **Address Book**, then clicking **Edit**.

Edit Address Book Entries

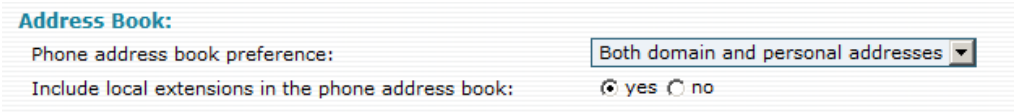
1. From the **Lists** tab, click **Address Book**.
2. Click the edit icon for the entry you would like to edit.
3. Make any necessary changes.
4. Click **Save**.

Delete Address Book Entries

1. From the **Lists** tab, click **Address Book**.
2. Click the delete icon next to the entry you would like to delete.

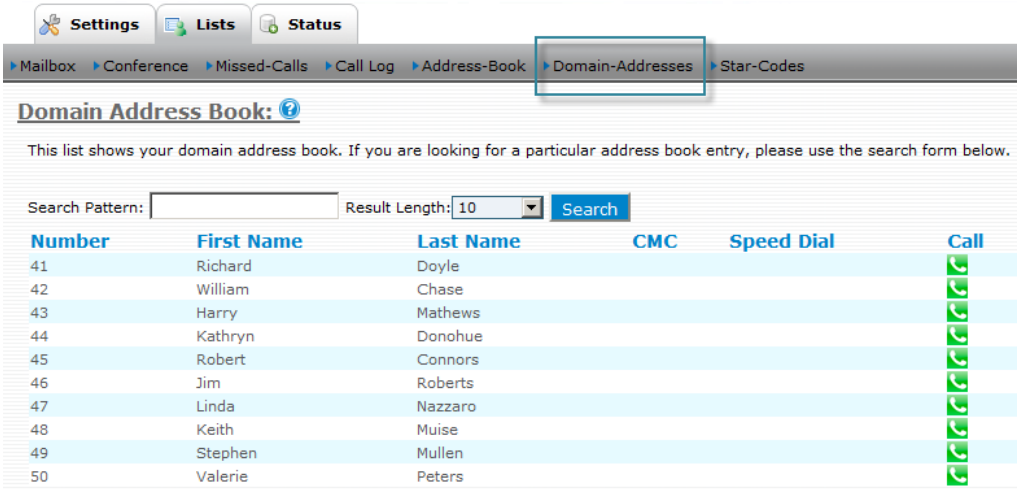
Upload Address Book to Phone

The administrator can enable the setting shown below so that users can upload both the personal and domain address books to their phone.



Domain Address Book

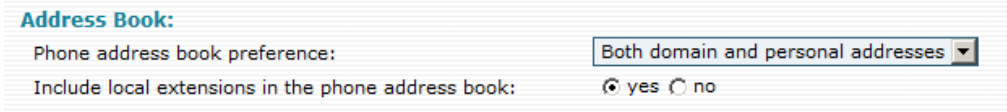
Domain address book entries are visible to and searchable by all members of the domain. Users can access the domain address book by going to **Lists > Domain-Addresses**:



The address book can also be used to indicate which DID number has been dialed. If the user adds an address book entry that matches a specific DID, the system will add the display name to the caller-ID and the phone can then display the text associated with the caller-ID.

Upload Domain Address Book to Phone

The administrator can enable the setting shown below so that users can upload both the personal and domain address books to their phone.



Extension Status

The **Status** tab shows the current status of the user's extension. It displays redirection settings, DND status, last number dialed, and many other settings. Users can view their status settings by clicking the **Status** tab:

The **Status** tab addresses the following settings:

- Do not disturb: This field will be set to `true` if the extension is on DND mode.
- Agent logged in: This field shows whether the extension is logged into an agent group.
- Hot Desking at: If the extension has redirected all calls (including calls from hunt groups and agent groups) to another location, the destination is shown in this line.

- Call forward all destination: If the **Call forward all calls** setting has been set, the destination is shown here.
- Call forward busy destination: If the **Call forward calls when busy** has been set, the destination is shown here.
- Call forward on no answer: If the **Call forward on no answer** setting has been changed, the destination is shown here.
- Timeout for **call forward on no answer**: If the **Call forward no answer timeout** has been changed, it will be indicated here.
- Timeout for mailbox: If the **Time until mailbox picks up** setting has been changed, the change will be indicated here.
- Call redial: This entry reflects the last number that was dialed from the user's extension. The **Redial a Number (*66)** star code can be used to redial the number.
- Call return: This entry reflects the last number that dialed the user's extension. The **Call Return (*69)** star code can be used to return the call.

Chapter 23

STAR CODES

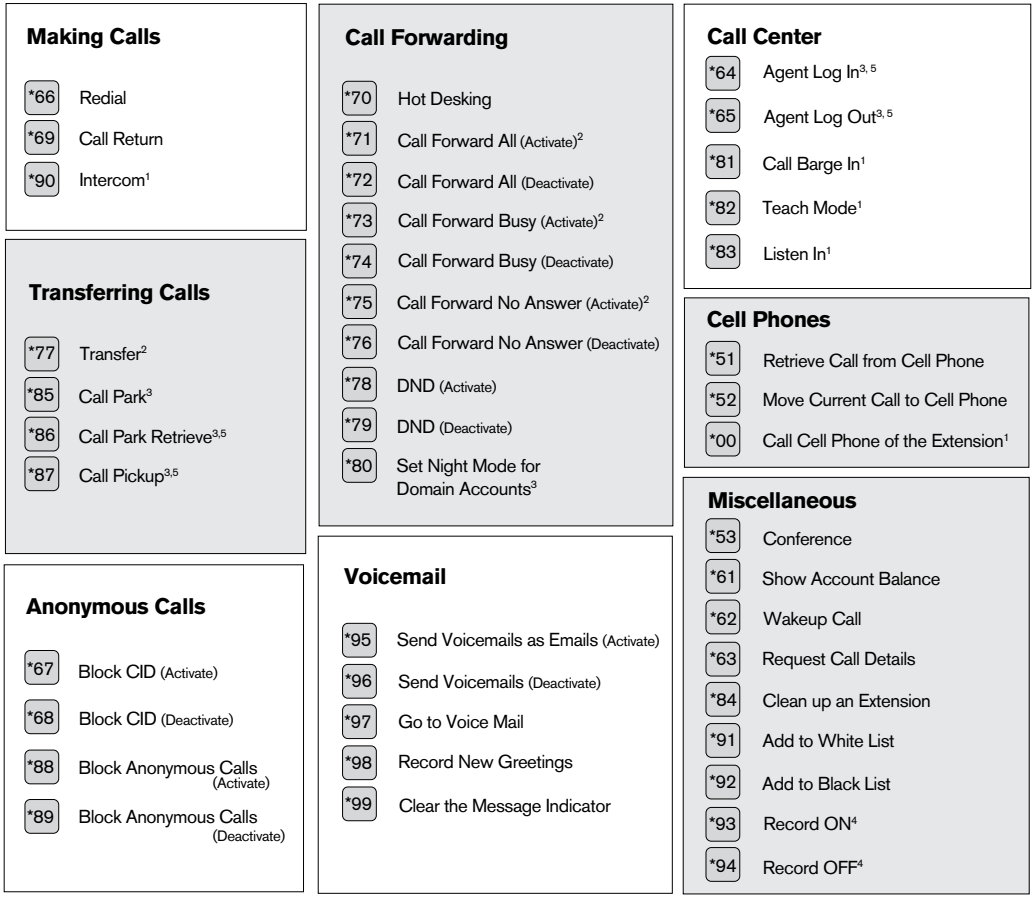
Star codes are two-digit numbers prefixed with a star (*) and are used to instruct the system. Each star code maps directly to an action of the system, allowing users to quickly access snom ONE features, such as Do Not Disturb (DND), call forwarding, and a host of other features. All users across the domain have access to the same set of star codes and can access the list by logging into their account and going to **Lists** > **Star Codes**.

This chapter provides instructions on how to use each star code with snom phones. In most cases, once the star code has been entered, the confirmation button (the confirm button) must be used to indicate that the dialing is complete.

Administrators may define their own plan for star codes, and for a few situations, the star codes will need to be modified. For example, when configuring an Agent Log In/ Agent Log Out toggle button, the star codes must be identical (e.g., *64/*64). This applies to Call Park and Call Park Retrieve also (e.g., *86/*86).

Star codes must begin with a star and include only two digits. Codes 01–60 are reserved for speed dialing.

Figure 23-1 displays the list of star codes that are available on snom ONE.



1. An extension number is required after these star codes.
2. A destination number (e.g., an extension or an external number) is required after these star codes.
3. An argument is optional for these star codes.
4. These codes are used during a conversation; the tones are audible and can be heard by the connected party.
5. These star codes must be identical to one another (e.g. *64/*64 and *86/*86) when configurated as a toggle button.

Figure 23-1. snom ONE Star Codes

Basic Star Codes

Redial a Number (*66)

Redial (*66) allows users to redial the last number that was called from their phone. The Call Log (page 420) can also be used to dial the last number dialed.

Call Return (*69)

Call Return (*69) will dial the number of the call that was received last. The number will be available until a call has been established to that number—not necessarily connected, which can help prevent users from calling back the same person twice. (If the user executes *69 and discontinues the call during its ring state though, *69 will not be able to access that number again unless the caller rings again.)

Notes:

If a user reaches an external mailbox, the system will handle the Call Return as if the call had been successfully established and will clear the number. If the user reaches a mailbox of another extension on the system, the Call Return number will not be cleared and the user will be able to make successive attempts at reaching that extension by dialing *69. The system will store a Call Return number only for calls that contain a valid caller-ID.

Telephones that share the same extension number will share the same redial and Call Return number.

The Call Log (page 420) can also be used to dial the last number received.

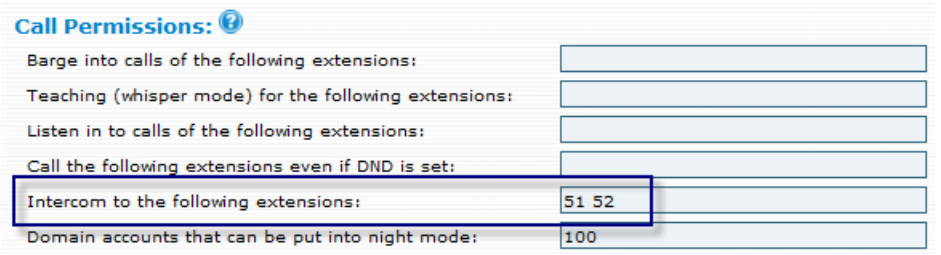
Intercom (*90)

The Intercom feature mimics the old secretary-boss intercom systems and can be thought of as a one-part page with two-way audio. Intercom is used to communicate

with one other person. The other party must have a separate extension number, as the Intercom feature will not work between two phones that are registered to the same extension. The Intercom feature will also not work when multiple registrations are involved with the receiving extension.

To activate:

1. Set the user's Call Permission settings for intercom (see page 174).


Call Permissions:
Barge into calls of the following extensions:
Teaching (whisper mode) for the following extensions:
Listen in to calls of the following extensions:
Call the following extensions even if DND is set:
Intercom to the following extensions:
51 52
Domain accounts that can be put into night mode:
100

2. Dial *90 and the extension you would like to intercom.
3. Press the confirm button on the telephone keypad.

You can now begin conversing with the other party.

Transferring Calls

Transfer Calls

Calls can be transferred using the **Transfer** button on the phone or star codes. The system supports two types of call transfers: blind transfer and attended transfer.

Blind Transfer

When the user activates a blind transfer, the call is transferred with no knowledge as to whether the receiving party will be available to receive the call. A blind transfer can be used for transferring calls to voicemail or the cell phone.

1. Press the **Transfer** button on your phone, or press **Hold** and dial *77.

2. Enter the extension number (or phone number) of the recipient.

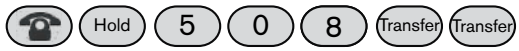
A blind transfer offers no confirmation of call connectivity. If the number is busy or does not exist or no one picks up, the user will not be notified.

Attended Transfer

When using attended transfer, the user must speak with the party who is receiving the call to ensure that the call can be received.

1. Put the caller on hold (using the phone's **Hold** button). The LCD will display the call that is on hold.
2. Enter the destination number.
3. Once the party on the receiving end is prepared to take the call, press the **Transfer** button *twice* (the first Transfer connects the call; the second Transfer clears the music so that the parties can speak. (If the phone does not have a **Transfer** button, *77 can be used to transfer the call.)

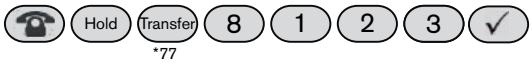
   Users do not need to press the **Hold** button to free the call. If the person is not available to take the call, the user can press the **Hold** button to reclaim the call and discuss the available options with the caller.



Transfer a Call Directly to Someone's Voicemail

The systems administrator must enable a direct dial prefix before users can "blindly" transfer a call to another user's voice mail. The default for direct dial is "8" (see page 100 for details on this setting).

1. Put the call on hold using the **Hold** button on your telephone keypad.
2. Press the **Transfer** key. (If your phone does not have a **Transfer** button, dial *77 to transfer the call.)
3. Enter the mailbox prefix number.
4. Enter the extension number.



The caller will be transferred to the extension's voicemail. Because the caller will bypass the voicemail timeout, the caller will not hear any ringing. This method does not need to involve an outside caller. To call a person's mailbox directly, the user can dial `8123`.

Call Park (*85) and Call Park Retrieve (*86)

Call Park allows the user to send a caller to someone whose whereabouts (within paging proximity) are not known. The receiving party uses Call Park Retrieve (*86) to retrieve the call.

Scenario: A call comes in for Diane, but you do not know where she it, so you put the customer on hold, dial `*85`, and press the confirm button. You then page Diane, "Diane, you have a call on extension 509" (509 is the extension on which the call was received). Diane executes the Call Park Retrieve (*86) feature, dials `509`, and retrieves the call. Park orbits can also be used for parking calls (rather than using your extension). When using a park orbit, enter the extension number of the park orbit after *85.

Park a call on your own extension

1. Put the call on hold (music plays in the background). If your phone does not have a **Hold** button, refer to the user guide that came with your phone.
2. Press *85 to park the call, then press the confirm button on your telephone keypad.

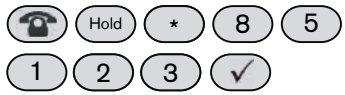
An announcement will indicate that the call has been parked. At this point, the call can be retrieved by any extension by dialing *86 and the extension number on which the call has been parked.

If the call is not picked up within a specified time (default is 1 minute), the user will receive a call from the system as a reminder of the waiting call.

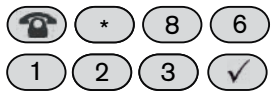
Park a call on a specific extension:

The system administrator may configure specific park orbits (e.g., 800, 801, 802, and 803) on the system so that all users can park calls to the same place. This is useful for monitoring parked calls and buttons, as well as for applications that need to park calls. Park orbits also ensure that voicemail does not pick up.

1. Put the call on hold (music will play in the background).
2. Press *85 to park the call.
3. Enter the extension number.



An announcement will indicate that the call has been parked. At this point, the call may be retrieved by any extension (which has permission) by dialing *86 and the extension number on which the call has been parked.



Call Pickup (*87)

Call Pickup allows users to pick up a ringing phone. It can be used to pick up calls ringing into a specific extension or for ringing calls in general, including calls ringing into a hunt group or agent group.

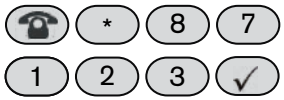
Note: When compared to Call Park Retrieve, Call Pickup is associated with a sense of urgency (i.e., the user must pick up the ringing phone before the call goes to voicemail.)

With Call Park Retrieve, the caller is already in the system, so there is not as much of a hurry.

Before users can use Call Pickup, they must first put their last call on hold so that the system does not interpret and execute the star key during calls made to external systems that also use star keys.

Directed Pickup

1. Dial *87.
2. Dial the extension on which the call is ringing.
3. Press the confirm button on the telephone keypad.



General Pickup

Call Pickup can also be used without specifying an extension. To activate, dial *87 and press the confirm button on the telephone keypad.

The system searches for calls to pick up in the following order:

- Hunt groups: For a call that is headed for a specified hunt group, the system will reroute the call to the extension that dials the pickup code. If several calls ring the hunt group, then the system will pick up only the first call that was routed to the hunt group.
- Extensions: When the account number is an extension, the system searches for calls that go directly to the specified extension. These calls can come from an auto attendant or through direct extension dialing. Calls that ring the extension due to it being part of a hunt group or agent group will not be affected by Call Pickup.
- Agent groups: As with the hunt group, the system picks up a call from the specified agent group. For calls in the ringing state, the system picks the first

call that is in that state. Otherwise, the system picks the call that entered the queue first.

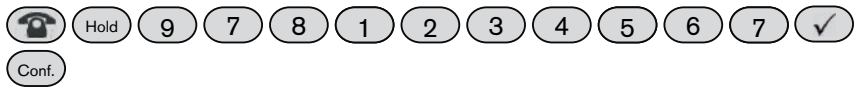
Conferencing

This section covers conference-related star codes and the three-way conference that users can be set up from the phone. For information on others types of conferencing, see Chapter 12.

Three-Way Conferences

Users who have **Hold** and **Conference** buttons can create a three-way conference using the phone:

1. Put the initial party on hold by pressing the **Hold** button on the phone.
2. Dial the extension or external number of the new party, and press the confirm button on the telephone keypad.
3. When the new party picks up, press the **Conference** button to merge the calls.



Note: This method of three-way conferencing may affect the network usage and call quality since numerous calls are being processed and merged together.

Conference (*53)

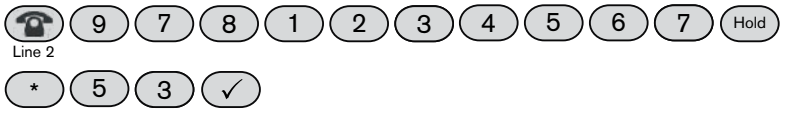
The Conference (*53) feature allows the user to quickly bring someone into an in-session conference, even though the person is not part of the participant list. The new party can be on a cell phone or regular phone. The benefit of this feature is that the new party is required to do nothing but answer the phone (conference number and access code are not needed). The party in charge of the conference simply needs to call the new party (from a line that is separate from the conference) and use *53 to join the party to the conference.

Scenario: You're in the middle of a conference call and you realize you need the input of someone who is not present in the conference. The individual happens to be traveling to a meeting, so you call the person on his cell phone and then connect him to the conference using the Conference feature.

To bring the party into the conference:

1. Call the party from a different phone line.

   (Use the ***00** feature if you need to access the individual's cell phone but do not know what that number is.)
2. Place the call on hold.
3. Enter *53, then press the confirm button on the telephone keypad.



Anonymous Calls

Block Caller-ID (*67)

Block Caller-ID (*67) allows users to keep their phone number and name hidden from the parties they call. It also prevents called parties from looking the user up in an address book and initiating a callback. Calls from one extension to another extension will not be affected by *67. These calls will always reflect the caller-ID.

1. Dial *67 and press the confirm button on the telephone keypad.

   The user will hear an announcement indicating that the caller-ID will be blocked for all future calls.

   Note: Caller-ID is always presented for internal calls.
2. Dial *68 to re-enable your caller-ID.

Reject Anonymous Calls (*88)

Users can reject anonymous calls by dialing *88 and pressing the confirm button.

To re-allow anonymous calls, users must dial *89 and press the confirm button.

Note: If a user has set Call Forward to busy condition (page 412), the system will forward anonymous calls to the designated destination (e.g., an assistant). This will ensure that the user's anonymous calls are screened before the user takes the call. If the user has not set Call Forward to busy, the system will announce to the caller that the call cannot be taken because of the blocked caller-ID.

Other options are available for handling anonymous calls, such as screening the calls or using the **Ask for name** setting (page 411).

Forwarding Calls

Call forwarding allows users to forward their calls to another number. Multiple methods are available for doing this.

Hot Desking (*70)

Hot desking can minimize the need for office space and is often used as a cost-reduction method. It allows multiple users to use the same desk and phone, although at different times. Hot desking can be used on a temporary or permanent basis. In either case, once the user activates the hot desking feature, all calls made to the user's extension (or as part of a hunt group or agent group) will be routed to the new extension or destination. Outbound calls from the hot desking phone will reflect the user's caller-ID.

It is not expected that other significant inbound traffic is routed to the originally registered extension. This fact suggests that offices use "virtual" and "real" extension numbers:

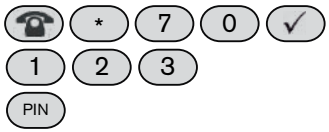
- Real extension numbers are used for employees with a fixed location (e.g., switch board, management).
- Virtual extensions are not registered. They are used simply for routing calls to a specific user.

Note: If users would like to route their calls to a colleague who is covering for the day, they can use either the Redirection star code (*71) or the redirection settings from the web interface (page 410).

To log into a hot desk:

Note: Users must set their voicemail **PIN** before they can use the Hot Desking feature.

1. Go to the phone where you will be hot desking.
2. Dial *70 and press the confirm button on the telephone keypad.
3. Enter your extension number when prompted.
4. Enter your voicemail PIN code for the extension number when prompted.

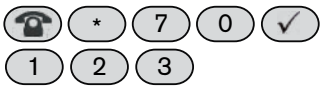


The system will acknowledge that the Hot Desking feature is in service.

Note: The system will automatically log a user out of a hot desk each night. Also, after activating the hot desk feature, users will be notified via email that a status change has been initiated on their extension.

To log out of a hot desk:

To log out of a hot desk, users must dial *70 and their extension number from either the location that is currently registered as a hot desk or from a phone that has been configured to their extension. The system will acknowledge that hot desking is no longer in service.

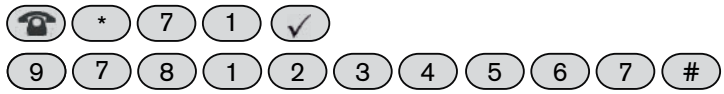


Note: Hot desking has limitations. Telephone preferences, such as ring tones, address book programming, etc., cannot be moved to another desk.

Call Forward All Calls (*71/*72)

The Call Forward All (*71) feature allows users to redirect all calls to another number (e.g., to a colleague who is answering the user's phone).

1. Dial *71 and press the confirm button on the telephone keypad.
2. Enter the call forwarding number once the announcement is complete.
3. Press the # key.



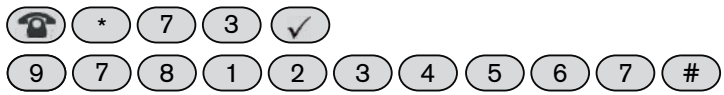
   The system will repeat the number and then hang up. If you want to change the forwarding number, just call *71 again.
4. To deactivate, press *72, then press the * key when prompted. The announcement will indicate that call forwarding has been turned off.

Users do not need physical access to their phone to modify this setting. This setting can also be activated from the web interface (page 411).

Call Forward on Busy (*73/*74)

The Call Forward on Busy (*73) feature allows users to forward calls to another number if their extension is busy. This feature is typically used for redirecting calls to a team member or colleague to ensure that all incoming calls are answered. To activate:

1. Dial *73 and press the confirm button on the telephone keypad.
2. Enter the call forwarding number once the announcement is complete.
3. Press the pound key (#).



The system will repeat the number and then hang up. If you want to change the forwarding number, just call *73 again.

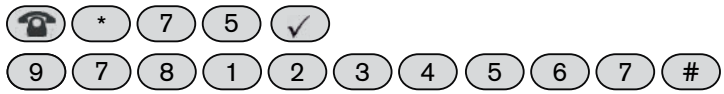
4. To deactivate, dial *74. The announcement will indicate that call forwarding has been turned off.

Users do not need physical access to their phone to modify this setting. This setting can also be activated from the web interface (page 412).

Call Forward on No Answer (*75/*76)

The Call Forward on No Answer feature allows users to redirect calls when the extension has not picked up after a certain time. This feature is typically used to redirect a user's incoming calls to an assistant or secondary phone. To activate:

1. Dial *75 and press the confirm button on the telephone keypad.
2. Enter the call forwarding number once the announcement is complete.
3. Press the pound key (#).



The system will repeat the number and hang up. If users want to change the forwarding number, they must dial *75 again.

4. To disable this feature, dial *76. The announcement will indicate that call forwarding has been turned off.

The length of time the system will wait before forwarding the call is determined by the **Call forward on no answer timeout** setting on page 101. Keep in mind that the voicemail timeout (see **Time until user's mailbox picks up** on page 98) works in tandem with the no-answer timeout. If the voicemail timeout kicks in before the no-answer timeout, the call will go to voicemail. Both of these settings can be set at the domain, but users can override these settings (page 413) if administrators have not blocked user access (Figure 2-6).

Do Not Disturb (*78)

Do Not Disturb or DND allows users to silence their phone for all incoming calls, even calls made to a hunt group or agent group. When DND is activated, all calls will stop, including those redirected to the cell phone. However, the system will still call the user's cell phone though if a message has been received while DND is activated *and* the user has activated **Call cell phone when new message arrives** (page 414).

1. To activate DND, dial *78 and press the confirm button on the telephone keypad.

2. Dial *79 to deactivate.

Notes:

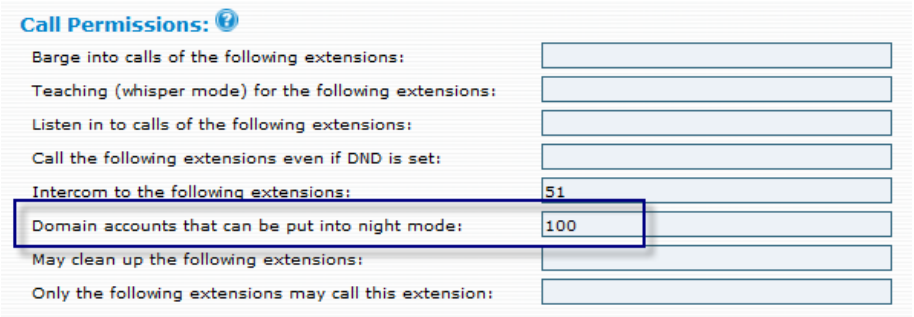
If the DND button on the phone is used to activate DND, this will not stop the user's cell phone from ringing. It will affect only that phone. To stop all phones from ringing, the user will need to activate the *78 star code so that the system will know to put all phones that have been configured to the extension into DND.

DND can be overridden by someone who has DND override permission. See **Call the following extensions even if DND is set** on page 174. Typically, this is a secretary who needs access to the boss, regardless of DND status.

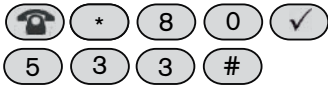
DND takes precedence over Call Forwarding, as the latter cannot prevent hunt group calls from reaching the user's extension.

Set Night Mode for Domain Accounts (*80)

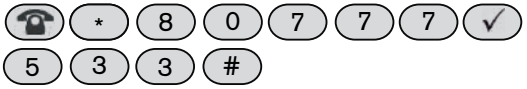
This feature allows users to forward domain accounts (e.g., auto attendant, hunt group, etc.) to their own extension. Before this feature can be used, permission for each account must be activated by the administrator. Permission is set from the extension's **Permission** tab (page 173).


Call Permissions:
Barge into calls of the following extensions:
Teaching (whisper mode) for the following extensions:
Listen in to calls of the following extensions:
Call the following extensions even if DND is set:
Intercom to the following extensions:
51
Domain accounts that can be put into night mode:
100
May clean up the following extensions:
Only the following extensions may call this extension:

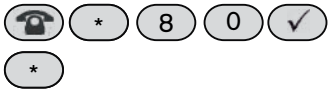
To forward all auto attendants, hunt groups, and agent groups of the domain, *80 must be used without an argument:



To forward only a specific account, the account must be specified after the star code:



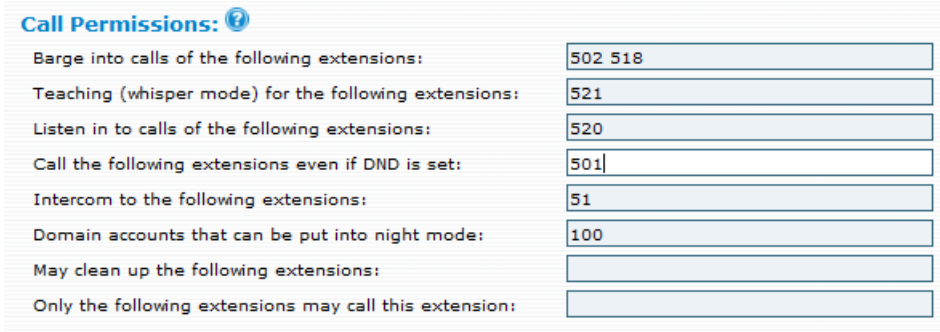
To disable this feature, enter a star in place of the call forward number:



Call Center Features

Call monitoring features must be used with caution. Please consult corporate and government regulations to determine whether these features are permitted in your environment. Illegal listening to phone calls is a severe crime, and system administrators must be aware of this.

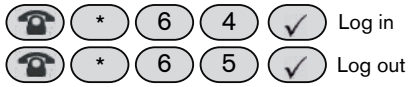
Many call center features are available only if extensions have been given permission to use them. These settings are controlled by the domain administrator and are located in the user's **Permission** tab (page 173).


Call Permissions:
Barge into calls of the following extensions:
502 518
Teaching (whisper mode) for the following extensions:
521
Listen in to calls of the following extensions:
520
Call the following extensions even if DND is set:
501
Intercom to the following extensions:
51
Domain accounts that can be put into night mode:
100
May clean up the following extensions:
Only the following extensions may call this extension:

Agent Log in/Log out (*64/*65)

The Agent Log In/Log Out star codes allow agents to log in and out of agent groups. Agents can use these codes to log themselves in at the beginning of a shift and then log back out when finished. Before agents can activate the log in/log out (*64/*65) features, agents must be given permission by the administrator. Agent groups are discussed in detail in 11.

To log out of all agent groups:



Agents who are members of numerous agent groups will need to specify which agent group they would like to log in or out of. Otherwise, they will be logged out of all agent groups. Using the sample shown below, the agent will be logged out of agent group 666 and will retain logged-in status for all other agent groups.

Call Barge (*81)

Call Barge allows a user to barge into an existing call between two people. Typically, the person barging into the call is either a secretary reminding the boss about another appointment or a co-worker in the next cube needing help on a call. Both parties can hear the third person come into the call and can hear the third person. Users cannot

activate Call Barge unless permission has been given by the domain administrator (page 173).

To activate Call Barge:

1. Dial *81 then enter the extension you would like to interrupt (e.g., *81508, where 508 is the extension).
2. Press start on the telephone keypad.

Call Teach Mode (*82)

Call Teach mode allows a third party to call into an existing call and communicate with one of the participants without the other person knowing. This is typically useful in a call center when a trainer wants to offer tips to a new agent without the customer knowing. This mode is sometimes referred to as "whisper mode" because the agent's phone must have an especially good echo cancellation so that the customer hears no background echo. Users cannot activate Call Teach unless permission has been given by the domain administrator (page 173).

To activate Call Teach mode:

1. Dial *82, then enter the extension number that should hear your voice.
2. Press the confirm button from the telephone keypad.

Listen In (*83)

Listen In mode allows a third party to listen in without being detected. The two parties speaking to each other are not notified about the listen-in and have no idea that a third party is on the phone. Users cannot activate Listen In unless permission has been given by the domain administrator (page 173).

To activate Listen In:

1. Dial *83, then enter the extension number that you would like to monitor.

2. Press the confirm button from the telephone keypad.

Miscellaneous

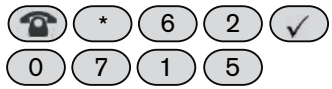
Show Account Balance (*61)

This feature allows users to hear the balance of their pre-paid calling card account. To get the balance, users simply enter *61 (followed by the confirm button) from the extension the pre-paid card is configured to. For more information on the pre-pay feature, refer to Chapter 16.

Wakeup Call (*62)

The Wakeup Call (*62) feature allows users to receive automatic wakeup calls from the system. Though this feature is used primarily in hospitality environments, it can also be used on an individual basis.

1. Dial *62.
2. Press the confirm button.
3. Enter the wakeup time in 24-hour format (HHMM); for example, `0715` (for 7:15 a.m.) and `1915` (for 7:15 p.m.).



The system will confirm the wakeup call. To cancel a wakeup call after it has already been confirmed, users must press the star (*) key.

Note: Wakeup calls cannot be transferred to other registered devices (i.e., the wakeup call will not ring the user's cell phone).

Request Call Details (*63)

The Request Call Details (*63) feature allows users to request the details of a call (caller-ID, call duration, and time of call). The information will be sent to the user's email address. This feature is handy and prevents the user from asking for contact information from the caller.

To activate the Request Call Details feature:

1. Dial *63 and press the confirm button on the telephone keypad.

2. Retrieve the message in your email.

Clean up an Extension (*84)

This feature allows users to quickly clean up an extension. This makes it ideal in hospitality environments, as it can be used to clear an extension of its messages after guests have checked out and before new ones arrive. It can also be used to clean up extensions of employees who have left the company. Users cannot activate this feature unless permission has been given by the domain administrator (page 173).

Add to White List (*91)

This feature allows users to add a contact to the white list of their personal address book. White list contacts receive preferred treatment. They are not required to say their name before speaking with the user, and they can receive a callback when the user's extension becomes available.

1. Dial *91.
2. Press the confirm button.

If the number does not already exist in the user's address book, the system will automatically create an entry for the number.

Users can edit the address book entry from the web interface (page 425).

Add to Black List (*92)

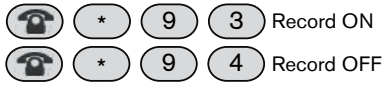
This feature helps users avoid unwanted contacts (e.g., unwanted callers, fax spammers, etc.). Once a caller is on the black list, the user's **Incoming anonymous call** setting will determine how that call is treated. If the caller should be rejected, then the system will reject that call. Otherwise, the system will carry out whatever instruction the user has configured. The **Incoming anonymous call** setting is detailed on page 411.

1. Dial *92.
2. Press the confirm button.

If the number does not already exist in the user's address book, the system will automatically create an entry for this number. Users can edit the address book entry from the web interface (page 425). Black list contacts are not allowed to camp on an extension.

Call Record (*93/*94)

Call Record allows users to record a conversation between themselves and another party. This feature is handy when it is critical that a user remember the contents of a particular call. Users should check state and federal laws before recording calls. To activate the record feature, dial *93 on the telephone keypad. To deactivate, dial *94.



The recording can be retrieved from the user's mailbox from the web interface (**Lists** > **Mailbox**), as shown below.

snom ONE
Home
Help
Logout
Settings
Lists
Status
Mailbox
Conference
Missed-Calls
Call Log
Address-Book
Domain-Addresses
Star-Codes
Mailbox of 50:
Time
Number
Duration
Flags
2010/09/12 07:16:02
Kelly Jones (51)
00:08
2010/09/12 07:57:31
Rachel Reed (50)
00:05
2010/09/12 07:57:49
Kelly Jones (51)
00:12
2010/09/12 07:58:04
Kelly Jones (51)

Chapter 24

VOICEMAIL

Following is a brief overview of what users can do with their voicemail account:

Table 24-1. Voicemail Features

Feature	Functionality
Multiple announcement modes	Users can choose which type of announcement callers will hear when calling their extension. Choices are anonymous announcement, name, or a personal greeting
Convenient voicemail accessibility	Users can access their voicemail from their desk phone, cell phone, or any external phone.
Voicemail timeout	Users can specify the number of seconds that their extension should ring before voicemail picks up.
Shared mailbox access	If the extension is being used as a group mailbox, all parties can access the voicemail from their own extension.
Cell phone notification of new voicemail	This feature allows users who have chosen not to forward calls to their cell phone to still receive a voicemail notification on the cell phone when a new message arrives.
Email notification of new voicemail	This feature allows you to receive your voicemail as email attachments.
Transfer a caller to another extension's voicemail.	If the systems administrator has enabled a direct dial number, users will be able to "blindly" transfer a call to someone else's voicemail. Because the caller will bypass the voicemail timeout, the caller will not hear any ringing.

Setting up the Voicemail Account

Changing the PIN

Users will need a voicemail PIN in several areas of snom ONE (e.g., when accessing their voicemail from an outside phone, when using the calling card feature, and when hot desking). Domain administrators can set a requirement for the minimum number of digits that users will be required to use for a PIN (see page 99). At least four or five digits is recommended. The PIN can be changed by the user as follows:

1. Dial extension number (if messages are waiting, press * to skip to the main menu).
2. Press **2**.
3. Enter new access code.
4. Press **1** to confirm.

Note: Users can also set their PIN from the web interface (page 407).

Record Your Name

This recording will be used in announcements to all callers. Users can choose not to record their name. The system will recite the extension number instead. The user's name can be recorded as follows:

1. Dial your extension number (if messages are waiting, press * to skip to the main menu).
2. Press **3**.
3. Begin recording your name.
4. Press the # sign.

   From here, users can listen to the recording (press 1), choose to use the recording (press 2), record again (press 3), or delete the recording and return to the previous menu (press 4).

Record a Personal Welcome Message

1. Dial extension number (if messages are waiting, press * to skip to the main menu).
2. Press **4**.
3. Record your personal greeting.
4. Press the # sign.

   From here, users can listen to the recording (press 1), choose to use the recording (press 2), record again (press 3), or delete the recording and return to the previous menu (press 4).

Accessing the Voicemail System

The main menu of the voicemail system is shown in Figure 24-1:

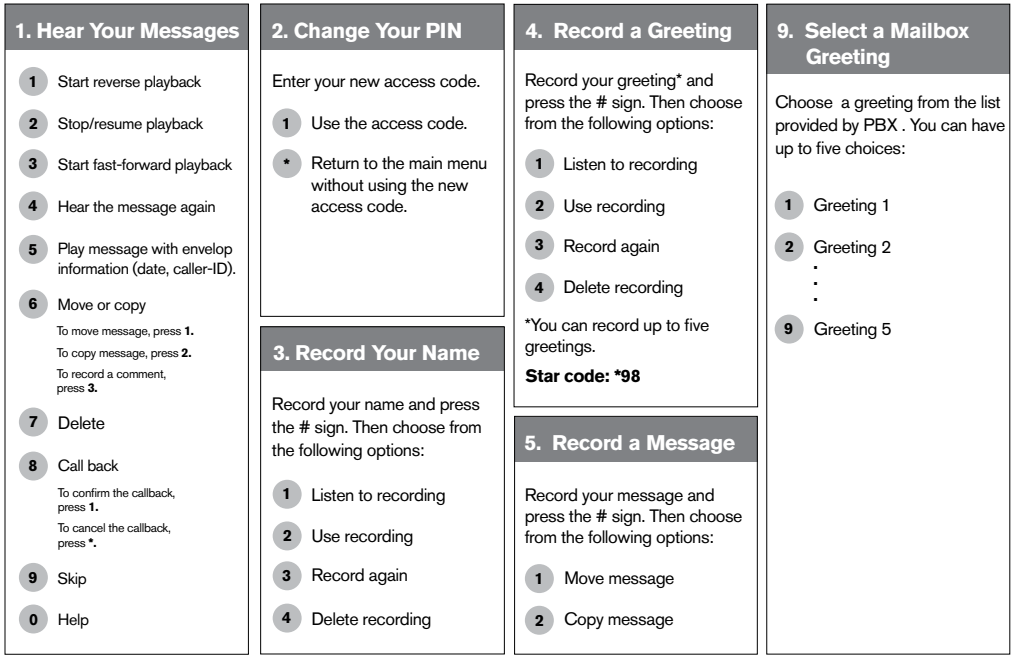

1. Hear Your Messages
1 Start reverse playback
2 Stop/resume playback
3 Start fast-forward playback
4 Hear the message again
5 Play message with envelop information (date, caller-ID).
6 Move or copy
To move message, press 1.
To copy message, press 2.
To record a comment, press 3.
7 Delete
8 Call back
To confirm the callback, press 1.
To cancel the callback, press *.
9 Skip
0 Help
2. Change Your PIN
Enter your new access code.
1 Use the access code.
* Return to the main menu without using the new access code.
3. Record Your Name
Record your name and press the # sign. Then choose from the following options:
1 Listen to recording
2 Use recording
3 Record again
4 Delete recording
4. Record a Greeting
Record your greeting* and press the # sign. Then choose from the following options:
1 Listen to recording
2 Use recording
3 Record again
4 Delete recording
*You can record up to five greetings.
Star code: *98
5. Record a Message
Record your message and press the # sign. Then choose from the following options:
1 Move message
2 Copy message
9. Select a Mailbox Greeting
Choose a greeting from the list provided by PBX . You can have up to five choices:
1 Greeting 1
2 Greeting 2
9 Greeting 5

Figure 24-1. Main Menu

Users can access the voicemail system using any of the following methods:

Listen to the messages from your main phone: Dial *97 and press the confirm button on the telephone keypad. (Another way to listen to your messages from your phone is by dialing your extension number.)

Listen to the messages from your cell phone: Dial into the main number and press 3 once you hear the auto attendant. The auto attendant will recite your messages and then deliver the prompts shown in Figure 24-1.

Listen to the messages from an outside phone:

1. Dial into the main number.
2. From the auto attendant, enter your extension number or if you know the direct dial prefix (8 is default), dial the prefix plus your extension (i.e., if your extension is 511, then enter 8511).
3. Press the star (*) key; otherwise, you will be prompted to leave a message.
4. Enter your voicemail PIN.

Example:

When users call their mailbox for the first time, they will be prompted to record their name. The recording will be used when someone calls their extension from the auto attendant. Users will also be prompted to record a greeting, which they can opt to use in place of their name. Once this has been established, anytime users call into their mailbox, the auto attendant will automatically recite their messages before delivering the prompts shown in Figure 24-1 (users can press the * key to skip their messages and go straight to the voice prompts).

Forwarding a Message

To forward a message to another recipient while listening to the message:

1. Press 6.
2. Press 1 to move the message to a single mailbox.
3. Enter the extension number.
4. Press #.

To copy a message to another recipient(s) while listening to the message:

1. Press 6.
2. Press 2.
3. Enter the extension number. When copying to multiple extensions, separate them by the # sign.
4. Press ## when finished.

Leaving Voicemail Messages

When users call another user, they have the option of receiving a callback (press 1) or leaving a message (press 2). Once they leave a message and press the # key, the options shown in Table 24-1 will be available.

Table 24-1. Options When Leaving a Voicemail Message

Key	Feature
1	Delete the message.
2	Record the message again.
3	Mark the message as urgent.
4	Mark the message as private.
0	Send the message and go to the operator.
9	Send the message and hang up.

Composing a New Message

Rather than leave a message directly on another user's voicemail, users have the option of composing a message and then moving it to another mailbox or copying it to multiple mailboxes.

1. Call into your voice mailbox.
2. If you have messages waiting, press * to skip to the main menu.
3. Press 5 from the main menu.
4. Record the message.
5. Press the # sign.

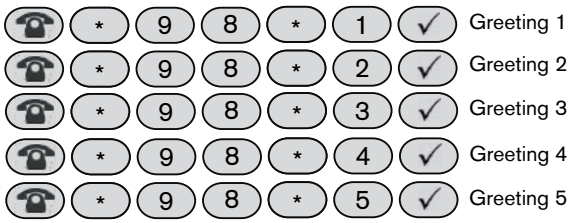
6. Select an action:
   - Press 1 to move the message to a single mailbox.
   - Press 2 to copy the message to one or more mailboxes. Use a # sign to separate multiple mailboxes.
   - Press 4 to mark as urgent.
   - Press 5 to mark as private.
7. Press ## when finished.

Personal Greetings

Users can record up to five individual greetings. Greetings will remain on the system and can be activated whenever users need them. See also Chapter 18 for detailed information on greetings in general.

Recording/Activating Personal Greetings

1. Dial *98 followed by the first greeting number (*1).
2. Press the Confirm button on the telephone keypad.



   If users need to re-record a greeting, they can activate the greeting and record again (i.e., dial *98*6 followed by the confirm button to re-record message 6).

   Greeting 0 is the initial greeting that was activated at the time the user set up the voicemail box.
3. To activate a greeting, users must dial their extension number, press 9, and select the greeting they want to use (* will bring the user to the main menu of the mailbox.)

Hearing Your Personal Greetings

1. Call into your voice mailbox.
2. Press * to skip to the main menu.
3. Press 9 from the main menu to hear your recorded greetings.

Advanced Features

Send a Voicemail Message Without Ringing Extension(s)

The voicemail system allows users to send voicemail messages to other users without ringing their extension. This is done by calling the voicemail system rather than the user's phone.

Scenario: Suppose two employees, Mary and Jack, are working on a project, and Mary has some information that Jack needs. Rather than phone him, she calls the voicemail system and records a message for Jack. She then tells the voicemail system to send it to Jack's extension. The message is immediately put into Jack's voice mailbox without his phone ever ringing. Jack's message waiting light immediately alerts him of a new message. The message can be sent to any number of additional employees.

To send a voicemail to multiple extensions without ringing extensions:

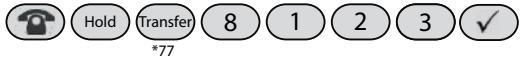
1. Enter your extension into the telephone keypad.

   This should bring you to the main menu of the auto attendant. If you hear your message instead, press the * key on the telephone keypad.
2. Press 5.
3. Record your message, then press the # sign.
4. Press 2 to copy the message to an extension(s).
5. Enter the extension(s). Multiple extensions must be separated by the # key. Press ## when finished.

Transfer a Call Directly to Someone's Voicemail

The system administrator must enable a direct dial number before users can "blindly" transfer a call to someone else's voicemail. The default for direct dial is "8."

1. Put the call on hold using the **Hold** button on your telephone keypad.
2. Press the **Transfer** key. (If your phone does not have a **Transfer** button, dial *77 to transfer the call.)
3. Enter the mailbox prefix key.
4. Enter the extension number.
5. Press the confirm button on the telephone keypad.



The caller will be transferred to the extension's voicemail. Because the caller will bypass the voicemail timeout, the caller will not hear any ringing.

This method does not need to involve an outside caller. If you want to call a person's mailbox directly, you can dial 8123 followed by the confirm button.

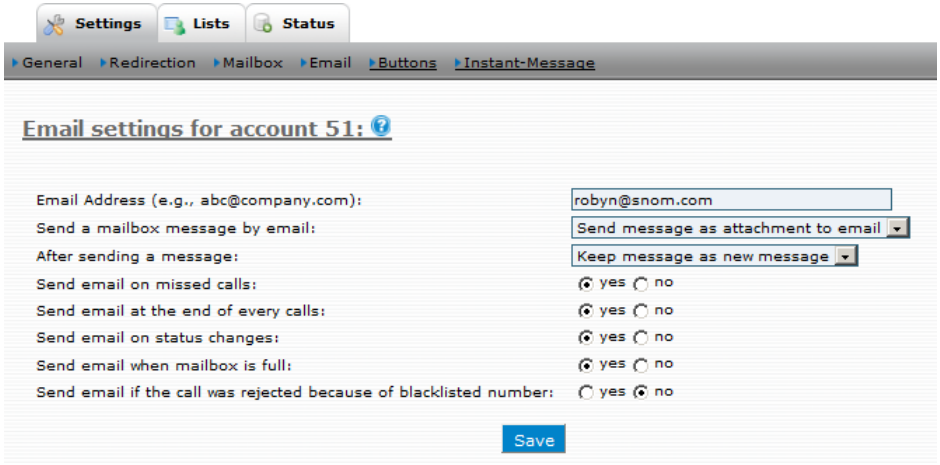
Listen to Voicemail on Cell Phone

Users can configure their account so that the system rings their cell phone whenever someone has left a voicemail. Even when DND has been activated, users will still be notified of new messages. For more information on this feature, see page 414.

Voicemail Notification

Via Email

Users can receive voicemails in their email account (as WAV files) by enabling the **Send message as attachment** setting (see page 416). Other settings are also available at this page (go to **Settings** > **Email**).



Via Cell Phone

If users have a cell phone (or another phone) configured to their extension, the system can alert them whenever a new message has arrived in their voicemail (see page 414). Even if the user's phone is on DND ("do not disturb), the system will call the second phone and let the user know that a new message is waiting.

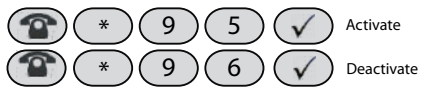
Voicemail Feature Codes

This section covers the handful of star codes that are associated with the voicemail system (*95, *96, *97, *98, and *99).

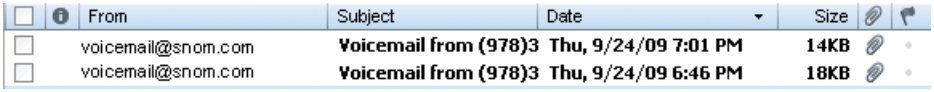
Send Voicemail to Email Account (*95/*96)

Users that have an email account on the system can have their voicemail forwarded to their email account. To activate this feature:

1. Dial *95 and press the confirm button on the telephone keypad.



Users can ask someone to leave a voicemail message to ensure that the forwarding works (the email is shown below). If they do not receive an email, they should check their spam folder.



Important: When using the *95 star code, users will *not* receive voicemails on their phone. All voicemails will be directed to their email account only. Users who prefer to receive voicemail messages on both their phone and email account should use the **Send a mailbox message by email** setting from the web interface (page 416).

Go to Voicemail (*97)

Users can listen to their voicemail from their phone by entering *97 and pressing the confirm button on the telephone keypad.

Users can also listen to their voicemail from an outside phone:

1. Dial into the main number.
2. From the auto attendant, enter your extension number or if you know the direct dial prefix (8 is default), dial the prefix plus your extension (i.e., if your extension is 511, then enter 8511).
3. Press the star (*) key; otherwise, you will be prompted to leave a message.
4. Enter your voicemail PIN.

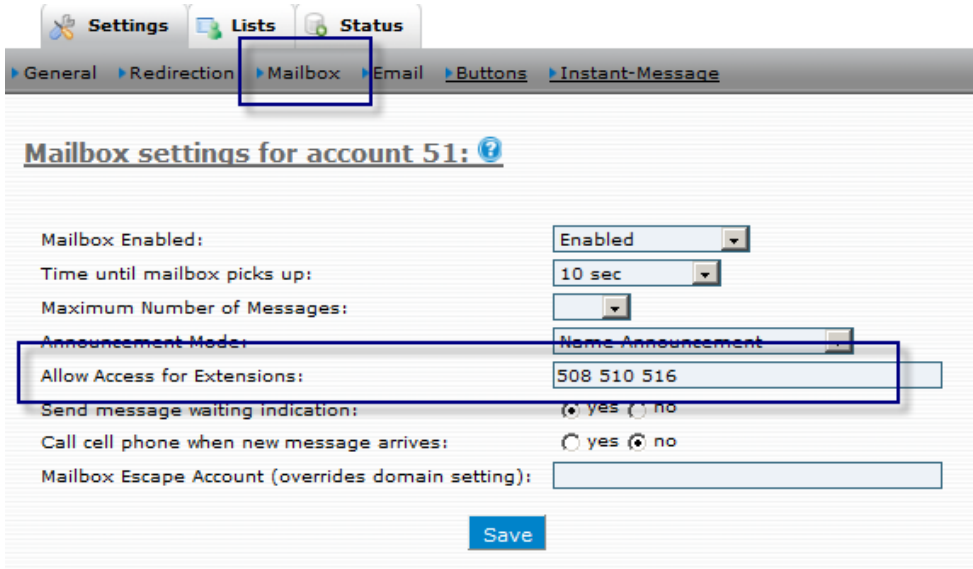
Go to Group Mail (*97)

Group mailboxes can be used for anything from a joint boss/secretary mailbox to a place to collect calls that come in after hours, at lunch, or during a holiday. Users that share a

mailbox with other users can access its voicemail messages in a way similar to accessing mail from a single user account.

Note: The messages that are left in the group mailbox can be picked up from either the user's extension or the group mailbox extension.

To create a group mailbox, the administrator needs to create an extension and enter the extensions of those who will be allowed to access the mailbox (see the **Allow Access for Extensions** setting shown below).



Users can listen to groupmail messages from their main phone by dialing *97 and pressing the confirm button on the telephone keypad.

☎ * 9 7 ✓

Users can also listen to groupmail messages from an outside phone:

1. Dial into the main number.
2. From the auto attendant, enter the extension number of the shared mailbox or if you know the direct dial prefix (8 is default), dial the prefix plus the extension (i.e., if the extension is 511, then enter 8511).
3. Press the star key; otherwise, you will be prompted to leave a message.

4. Enter the voicemail PIN of the shared mailbox.

Example:

Clear Message Waiting Indicator (*99)

The message waiting indicator (MWI) notifies the user through the message light on the phone when a new message has arrived. Depending on the type of phone the user has, the light will be either yellow or red. For all phones, the light will blink when a new message has arrived. Once the user has listened to the message, a solid light will replace the blinking light. This enables the system to alert the user the next time a new message has arrived.

Users can clear the message indicator without listening to their messages by dialing *99. (This will not delete their messages; it will only clear the indicator.)

Note: Users must activate the **Send message waiting indication** setting (page 414) to be notified of new messages.

Chapter 25

CELL PHONES

One of the most valuable benefits of cell phone integration is the ability to receive calls regardless of where you are without having to worry about unwanted ringing during off hours. Users can define which hours of the day or night they want to receive calls. Whether the phones ring simultaneously or in sequence, or whether the cell phone rings at all, is also controlled by the user.

The cell phone is treated like a registered IP phone. When calls come in, the system dials both the cell and desk phones. Cell phone integration gives the user numerous advantages, including lower cell phone costs and access to snom ONE star codes. Because the system recognizes the user when calling into the system from the cell phone, the user can easily access the Personal Virtual Assistant (page 473). Advantages of cell phone integration are highlighted in Table 25-1.

Table 25-1. Cell Phone Features

Feature	Functionality
Simultaneous ring	Cell phone integration enables the user to specify another phone number that will ring at the same time as the extension. This could be a cell phone or any other number.
Calling schedule	Users can set their own calling schedule. This schedule determines when the cell phone will respond to office extension calls.
Ring delay	Ring delay determines how long the office extension will ring before the cell phone redirection takes place. This is helpful if the user is in and out of the office throughout the day.
Safety net for office phone	If the extension is disconnected from the system at any time, calls will automatically be sent to the user's cell phone. When reconnected, the extension will resume ringing.

Note: Cell phone integration is different from having two phones registered to the same extension. Registering two phones to the same extension allows users to merely receive calls at one of two locations, while cell phone integration allows users to receive calls at any location, as well as be reached at numerous phone numbers. Cell phone configuration allows users to be accessible at all times, even in the event of a power failure. If the office extension (or remote extension) is disconnected from the system, calls will automatically be sent to the user's cell phone. Once the phone is reconnected, incoming calls will automatically be rerouted to the extension.

Figure 26-1 illustrates the role that the cell phone plays in handling an incoming call. First, the cell phone must be configured to be included in all calls. Next, the call rings both phones. In the event the user decides not to answer the call, the caller can leave a message. Users have numerous options for listening to the message.

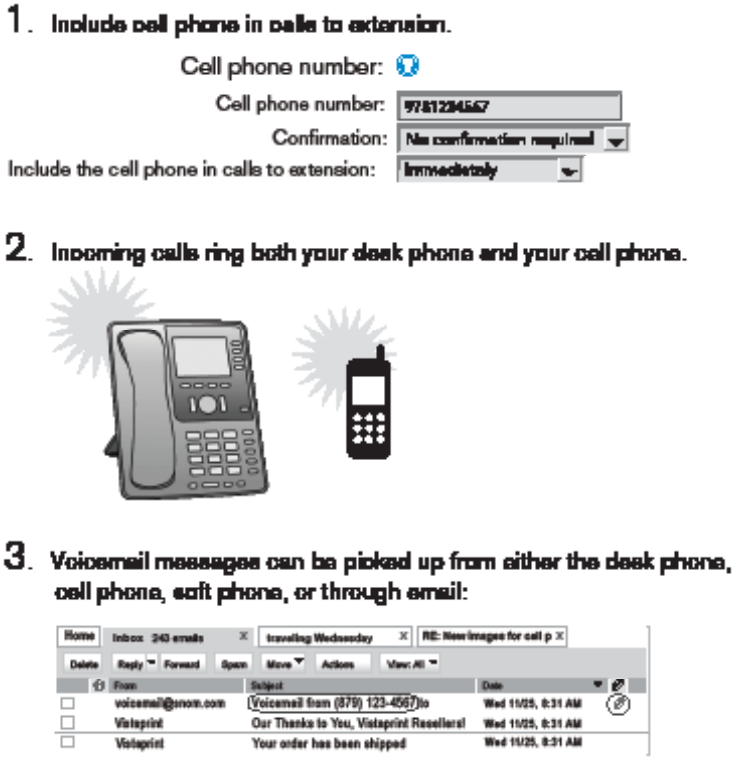


Figure 25-1. Cell Phone Integration in Action

Cost Savings

Once the user's cell phone has been integrated to the extension, the callback feature can be used to reduce the costs of international dialing. (The callback feature is also available through the calling card account.)

Callback

The callback feature is ideal from not only a cost savings perspective but also from a billing perspective. Users can call into the system to request a callback from any destination they designate. Regardless of where each call is made from and to, all calls will be listed in the same account. Single-location billing allows employees who work from home to keep their personal lines separate from their business calls.

This feature is designed for users making calls from international destinations back to their home country. Neither the user nor the party receiving the call will be charged for the call. The call will be charged to the user's extension. If the user has a cell phone plan that charges only for outbound calls, international calls will be free if placed using the callback feature.

Note: The callback feature can be used from a phone that has not been integrated to the user's account (e.g., a phone from the user's hotel room); however, it is much simpler from a phone that is registered.

Request a Call Back

Once the user's cell phone has been integrated as part of the user's extension, the callback feature is easily accessible through the Personal Virtual Assistant and requires neither an extension number nor a PIN when the callback is initiated.

1. Dial into the system. The Personal Virtual Assistant announces the options.
2. Press 2 to initiate the callback.

   The phone will be silent for approximately 30 seconds before the system calls you back.
3. Enter the destination number followed by the # sign. The system will connect the call, billing both calls to the user's extension number.

Calling Card Account

Before users can use the calling card, they need to know the extension number of the account (see your administrator). A calling card account can can be used in numerous ways:

- As a standard calling card to reach out to a third-party web server for call authentication and pin use.
- To dial into the system and have the system dial out.
- To dial into the system and request a callback.

The calling card is ideal when traveling because it allows users to place outbound calls from the system without logging into their extension. And regardless of where they are calling from, users can present the caller-ID of their office (they can also block their caller-ID).

The calling card allows users to make international calls at much lower rates than if dialing the calls directly. For example, dialing the Caribbean from the United States costs in excess of $1.00 per minute if dialed directly. With the calling card and SIP trunking, it could cost as little as $0.20 per minute.

Initiating a Callback Using the Calling Card Account

A calling card account enables users to call into the system from a phone that has not been configured to their account and initiate a callback.

1. Dial into the calling card system using the main number.
2. The auto attendant announces the options.
3. Enter the extension number of the calling card account.
4. Enter your extension number.
5. Enter your PIN.
6. Enter the destination number followed by the # sign (a phone number or an extension number is allowed).

   The system will connect the call, billing the call to the user's extension.

Once the user's cell phone has been configured to the extension, the user can use the calling card to make these calls from the cell phone. Although calls made using the

calling card still consume the user's cell phone minutes, the rates are less expensive than calling directly. Users can view calls placed from the calling card by going to **Lists** > **Call Log**.

Configuring the Cell Phone

Add a Cell Phone to Your Account

This section shows you how to configure a cell phone to the account. Navigate to **Settings** > **Redirection**. Details for each setting are shown after Figure 25-2

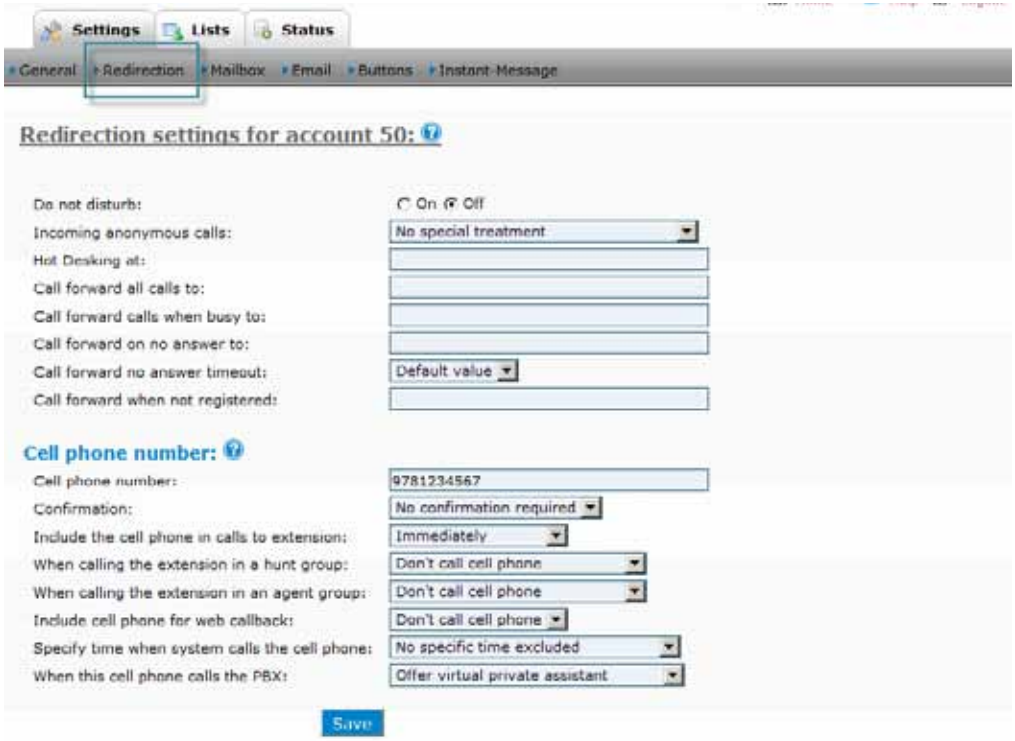
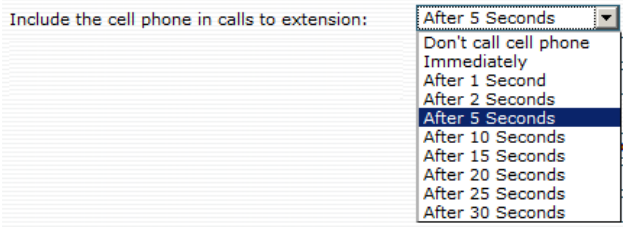


Figure 25-2. Cell Phone Settings

- **Cell phone number**: While most users populate this field with a cell phone number, any phone number can be used. The number should be entered without any spaces or hyphens (e.g., 9781234567).

- **Confirmation**: This setting allows users to require confirmation (i.e., pressing 1 on the cell phone) before the call will be connected. The benefit of requiring confirmation is that if the cell phone is temporarily unavailable (i.e., out of range, without power, etc.), the call will not automatically go to the user's voicemail and the caller is likely to call back.

- **Include the cell phone in calls to extension**: This feature gives users the freedom to pick up calls from either their extension or cell phone. When this feature is activated, both phones will ring. Call forward rings only the phone where the call is being redirected to. The cell phone can be set to ring from 1 to 30 seconds after the extension starts ringing.



- **When calling the extension in a hunt group**: This setting allows users to tell the system to include their cell phone in calls made to a hunt group.
- **When calling the extension in an agent group**: This setting allows users to tell the system to include their cell phone in calls made to an agent group.
- **Include cell phone for web callback:** This setting is linked to the click-to-dial feature which is available from the address book, missed calls, and call log pages. Click-to-dial works as follows: A user clicks a contact, and the system calls the user's extension before it dials the contact. The **Include cell phone for web callback** setting allows the user to include a cell phone in the mix. When this setting is set to **on**, the system will call both the extension and the user's cell phone. After one of the phones is answered, the PBX dials the contact. This setting is useful if the user is traveling and does not have access to the office phone.

- **Specify time when system calls the cell phone**: The options within this setting allow users to specify the times at which the system will ring their cell phone. This setting can prevent calls in the middle of the night.

  Note: The user's time zone setting must be set to reflect the user's time zone; otherwise, calls may be received outside the parameters set for the cell phone.

  Users have the following options when configuring their cell phone:

  – **No specific time excluded**: The cell phone will ring every time the user's extension rings, regardless of the time.

  – **Explicitly specify available times**: This setting allows a user to specify a schedule for the system to use when calling the cell phone (Figure 25-3). Users must populate the fields for each day of the week.

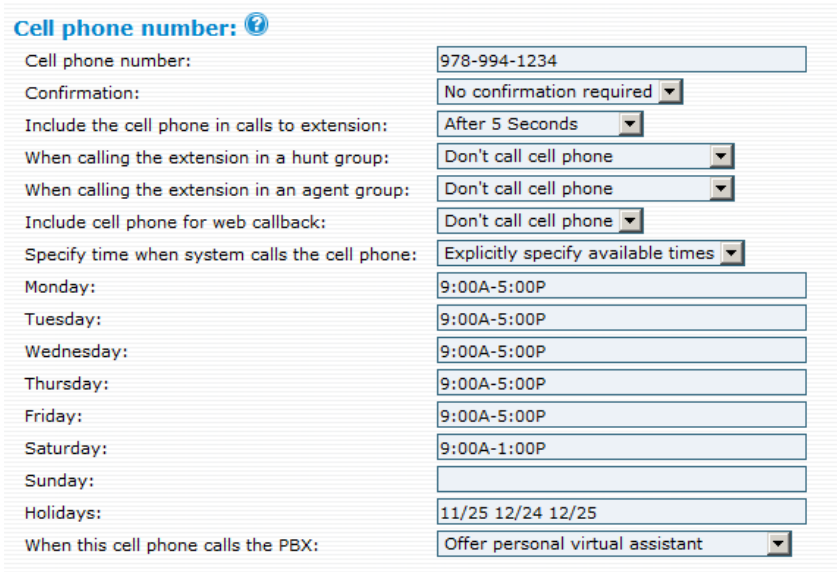


Figure 25-3. Cell Phone Calling Schedule

  - Users can use either the 24-hour format (e.g., 21:00 for 9:00 p.m.) or the English AM/PM style (e.g., 9:00P for 9:00 p.m.). However, both formats require a start time and an end time (e.g., HH:MM-HH:MM).

- To specify more than one time segment, the following format must be used: 9:00-12:00 1:00P-7:00P (one space separates the two segments).
- To specify the days on which the schedule should *not* be activated, such as a holiday or any other day, the holiday field must be used:
  - To specify 1 day, use the MM/DD format (e.g., 11/24 for November 24).
  - To specify 2 days, use the MM/DD format with a space between the days (e.g., 12/24 12/25 for December 24 and 25).

- **When this cell phone calls the PBX:** The Personal Virtual Assistant (page 474) provides special prompts to users who call into the system from their cell phone. This setting allows you to turn this feature off.

When this cell phone calls the PBX:
Offer personal virtual assistant
Offer personal virtual assistant
Do not offer personal virtual assistant

Safeguard Against Loss-of-Signal Events

In the event of a power outage (or if the user's phone has been turned off), incoming calls will typically be terminated on the voicemail of the cell phone. To prevent missing calls in this way, users can activate the Confirmation feature so that the system will wait *until the user accept the call* (by pressing 1) before actually connecting the call. The system will not send the call to voicemail. This way, the caller is likely to call back. Users can configure this setting by selecting **Press "1" to connect the call** as shown below:

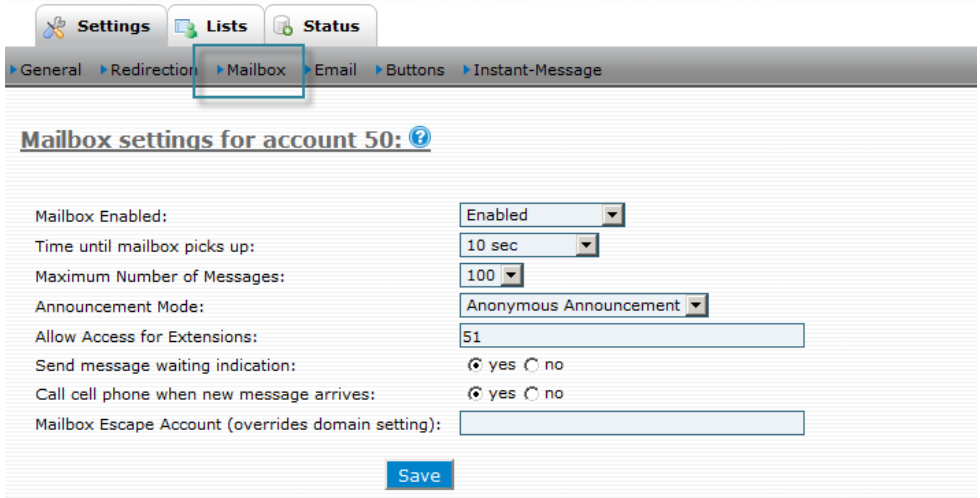
Ring My Cell Phone When Voicemail Arrives

If users have decided against forwarding their calls to their cell phone but still want to be alerted when a new message arrives on their extension, they can receive a call on

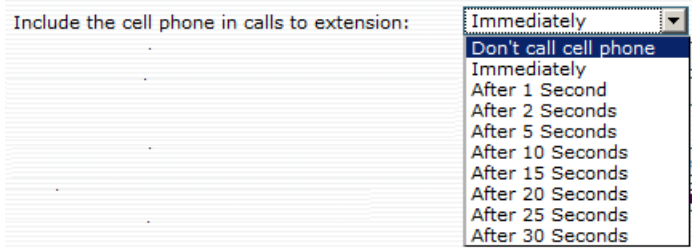
their cell phone when someone has left a message. Once a caller has left a message, the system will call the user on the cell phone. The user can press 1 to pick up the message.

To activate this feature:

1. From the **Settings** tab, click **Mailbox**. Then click **Yes** to activate the **Call cell phone** feature as shown below:



2. Tell the system not to include your cell phone in any incoming calls. To do this, modify your cell phone redirection settings, as shown below:



Note: Putting your phone into DND mode (using *78) will prevent incoming calls from ringing your cell phone; however, you will be notified of new voice-mail messages as long as you activate the **Call cell phone** setting.

Feature Codes

The feature codes used in this section are related to cell phone use (*51, *52, or *00) but they cannot be executed *from* the cell phone.

Retrieve Call From Cell Phone (*51)

This feature allows users to pick up an in-process cell phone call on their extension phone. This feature can be used only for calls that have been made from the cell phone (through the Personal Virtual Assistant) or which have been redirected to the user's cell phone. Calls that have been made directly to the user's cell phone (without involving the system) cannot be picked up on the user's extension phone.

Scenario: You're on your way to the office and you need to call a client, so you call into the system and place an outbound call. You speak with the client on your way to work, and once you arrive at the office, you decide to pick the call up from your office phone.

To transfer a cell phone call to your extension:

1. From your cell phone, call into the main number of the PBX (your cell phone must be associated with your account).
2. From the Personal Virtual Assistant menu, press 1 for "outbound call."
3. Enter a destination number, then press the # key.
4. When you're ready to pick the call up from your office phone, dial *51 from the office phone.

   Once the call has been connected, your cell phone will disconnect and will no longer accumulate minutes.

Move Current Call to Cell Phone (*52)

This feature allows users to move a current call from the extension phone to the cell phone. (*Note*: The user's cell phone must be configured to the extension before this feature can be used.)

Scenario: You're on your extension in the middle of a conversation and need to leave the office. Instead of ending the conversation, you put the caller on hold and transfer the call to your cell phone.

To transfer an extension call to your cell phone:

1. Place the extension call on hold.
2. Dial *52 from your office phone.
3. Answer the call on your cell phone.

Call Cell Phone of the Extension (*00)

This feature allows users to call someone else's cell phone *without* knowing that person's cell phone number. (*Note*: The individual's cell phone number must be configured as part of the extension that is being called.)

Scenario: You notice that your boss has just left the building when an important call comes in. You have no idea what his cell phone number is, but you must speak with him. You know what his extension number is, so you use the *00 star code followed by his extension number. Because the system sees the extension and the cell phone number as being the same, the system is able to ring his cell phone.

To call someone's cell phone without knowing the number:

1. Dial *00 followed by the person's extension number.
2. Press the start button from the telephone keypad.

The system will connect you to the individual's cell phone.

Personal Virtual Assistant

Once a user's cell phone has been configured as part of the extension, the system will recognize the user when the user call into the system from that phone. Instead of hearing the auto attendant, the user will hear the Personal Virtual Assistant, which will present the user with a new set of prompts. These prompts allow the user to make outbound calls, receive callbacks, go to voicemail, or go to the auto attendant.

Note: Administrators can disable the Personal Virtual Assistant using the **When this cell phone calls the PBX** setting (page 470) if the auto attendant is preferred instead.

To access the Personal Virtual Assistant:

1. From your cell phone (or another phone that has been configured to your extension), call into the system and press 3 ("Go to your mailbox").
2. At anytime during the announcement, you can enter a star code. For example, to set call forwarding, use *71 (call redirection) and enter a call forwarding number. In this example, all calls will be forwarded to 781-123-4567.

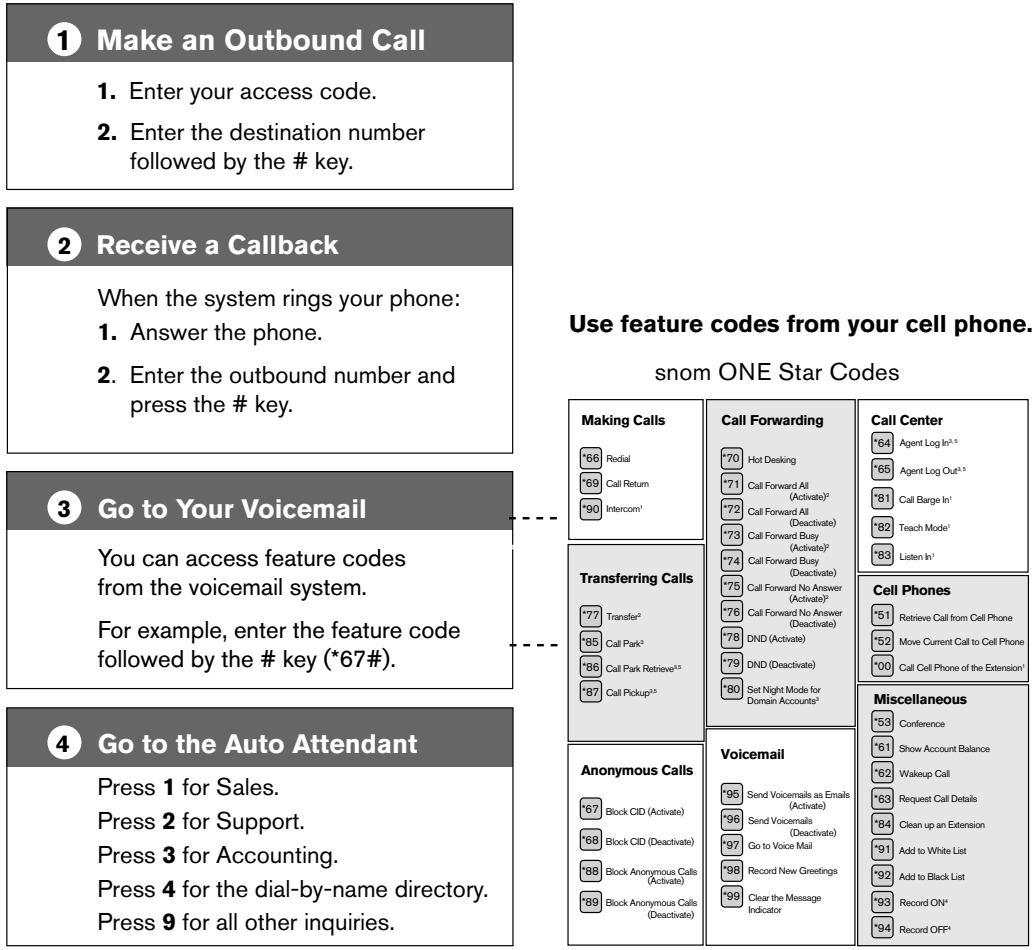

1 Make an Outbound Call
1. Enter your access code.
2. Enter the destination number followed by the # key.
2 Receive a Callback
When the system rings your phone:
1. Answer the phone.
2. Enter the outbound number and press the # key.
3 Go to Your Voicemail
You can access feature codes from the voicemail system.
For example, enter the feature code followed by the # key (*67#).
4 Go to the Auto Attendant
Press 1 for Sales.
Press 2 for Support.
Press 3 for Accounting.
Press 4 for the dial-by-name directory.
Press 9 for all other inquiries.
Use feature codes from your cell phone.
snom ONE Star Codes
Making Calls
*66 Redial
*69 Call Return
*90 Intercom1
Transferring Calls
*77 Transfer2
*85 Call Park3
*86 Call Park Retrieve3,5
*87 Call Pickup3,5
Anonymous Calls
*67 Block CID (Activate)
*68 Block CID (Deactivate)
*88 Block Anonymous Calls (Activate)
*89 Block Anonymous Calls (Deactivate)
Call Forwarding
*70 Hot Desking
*71 Call Forward All (Activate)2
*72 Call Forward All (Deactivate)
*73 Call Forward Busy (Activate)2
*74 Call Forward Busy (Deactivate)
*75 Call Forward No Answer (Activate)2
*76 Call Forward No Answer (Deactivate)
*78 DND (Activate)
*79 DND (Deactivate)
*80 Set Night Mode for Domain Accounts3
Voicemail
*95 Send Voicemails as Emails (Activate)
*96 Send Voicemails (Deactivate)
*97 Go to Voice Mail
*98 Record New Greetings
*99 Clear the Message Indicator
Call Center
*64 Agent Log In3,5
*65 Agent Log Out3,5
*81 Call Barge In1
*82 Teach Mode1
*83 Listen In1
Cell Phones
*51 Retrieve Call from Cell Phone
*52 Move Current Call to Cell Phone
*00 Call Cell Phone of the Extension1
Miscellaneous
*53 Conference
*61 Show Account Balance
*62 Wakeup Call
*63 Request Call Details
*84 Clean up an Extension
*91 Add to White List
*92 Add to Black List
*93 Record ON4
*94 Record OFF4

Figure 25-4. Personal Virtual Assistant

snom ONE

Appendices

Appendix A

WORKING WITH CSV FILES

CSV (comma-separated values) files can expedite the creation of all types of accounts, as well as the domain address book. A CSV file is a plain text file that stores tabular data from database-style tools. Records appear on separate lines, and the fields within each record are traditionally separated by commas (snom ONE uses semicolons). Once the CSV file has been created, it must be uploaded through the **Import CSV** account type from the **Accounts** tab, as shown below:

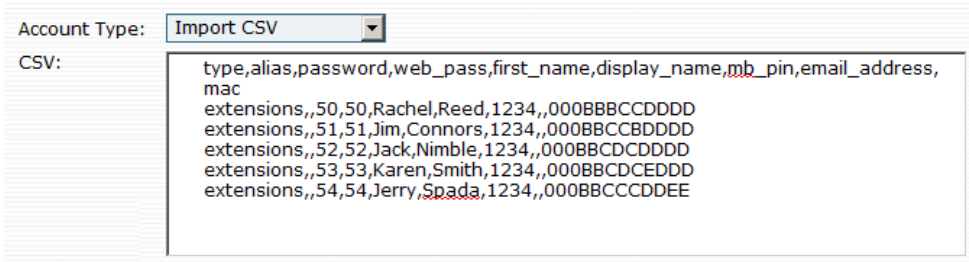


Figure 27-1. CSV Data Pasted into snom ONE

CSV files can be created from many document types, including Excel and Word. They can also be created from scratch (i.e., entering the data directly into Notepad or into the CSV field as shown above). This document uses an Excel file as the file type to illustrate the steps.

Structural Requirements

The first step in any conversion process is knowing the file requirements and determining the parameters you need for a particular account. This information is detailed on the following pages.

Structure

CSV files need to follow to the structural requirements that have been set by snom. For example, if you are preparing a file for an address book import, it cannot include fields that are not part of snom ONE's address book structure. Extra columns (e.g., "Nick Name," as shown below) will need to be removed.

```
First Name;Last Name;Nick Name;Phone;Speed Dial
First Name;Last Name;Phone;Speed Dial
```

Other requirements are listed below:

- The first line of your CSV file requires a "header." The header specifies which fields will be used and can include only the acceptable parameter names (lowercase letters are required).

```
First Name;Last Name;Phone;Speed Dial      Incorrect syntax
first_name;display_name;number;speed       Correct syntax
```

- Each record must be on one line (lengthy records can wrap onto the next line). When lines do wrap, be sure to surround the field containing the embedded line-break with double-quotes.
- Fields must be separated with semicolons. During CSV file conversions, commas are automatically used to separate the fields. Before importing the file to snom ONE, replace the commas with semicolons.

```
Smith,Mary,9783731234      Incorrect syntax
Smith;Mary;9783731234      Correct syntax
```

- Fields with embedded semicolons must be delimited with double-quotes.
- Fields that contain double quote characters must be surrounded by double-quotes, and the embedded double-quotes must each be surrounded by a pair of consecutive double quotes.

```
Company "A,B,C"            Incorrect syntax
"Company ""ABC"""          Correct syntax
```

For most files being converted to CSV, the two criteria that usually need to be addressed are the file structure and the field separator (the comma changes to a semicolon).

The following four lines meet the criteria stated above: Records are on separate lines, semicolons act as field separators, and embedded quotes have been addressed.

```
Cynthia Smith;102 Tremont Street;Bradford;MA;01834;9781234567
Bob Pine;22 King Street;Boston;MA;02134;6171234567
Cathy Chere;13 Tremont Street;Bradford;MA;01834;9781234567
Pat Rushetta;18 Elm Street;Bradford;MA;01834;9781234567
"Company ""ABC""";38 Main Street;Boston;MA;02134;6171234567
```

Parameters

This section outlines the parameters that are used most often when creating the different snom ONE account types. The only parameters that are required for any account are `alias` and `type`. (Address books are discussed on page 493.)

Extensions

Not all parameters listed in Table A-1 are required, with the exception of `alias` and `type`. Parameters can be added or removed based on need, and not every extension will necessarily have a value for every parameter you've included. In those cases, be sure to retain the semicolon (;) for that field so that the number of values in each line correlates with the number of parameters in the top line. For example, the first line below shows a missing ANI, and the line following it shows two semicolons to make provision for this missing field.

```
type;alias;ani;password;web_pass;first_name;display_name;mb_
pin;email_address;mac
extensions;651;;1234;1234;Carl;Clever;1234;cc@abc.
com;000BBBCCCDDDE
```

Table A-1 Extension Account Parameters

Parameter	Definition	Value
type	Account type	`extensions`
alias	Extension number and alias	`508 Johnny*`
ani	ANI	
password	SIP password	`1234`

Parameter	Definition	Value
web_pass	Web interface password	1234
first_name	User's first name	John
display_name	User's last name	Smith
mb_pin	User's PIN	1234
email_address	User's mail address	
mac	User's MAC IP address	192.168.1.4
picom	Extensions permitted to barge in	509 509 *
profile	Button profile for this phone	12-button

*When aliases are used in the CSV file, they will show up on the accounts page as a separate entry, giving the impression that each extension has been created twice. While this will not be a problem, you can avoid this by entering aliases manually once the account has been created.

Sample Syntax—Extension

```
type;alias;ani;password;web_pass;first_name;display_name;mb_
pin;email_address;mac
extensions;650;9786501234;1234;1234;Fred;Feuerstein;1234;
ff@abc.com;000BBBCCCDDDD
extensions;651;9786511234;1234;1234;Carl;Clever;1234;cc@
abc.com;000BBBCCCDDDE
```

Agent Groups

The parameters for the agent group are listed in Table A-2 (only *type* and *alias* are required).

Table A-2 Agent Group Parameters

Parameter	Definition	Value
type	Account type	acds
alias	Extension number of the agent group	663
agents	Extension numbers of the agents	41 42 43

Parameter	Definition	Value
gap_time	The number of seconds that the system should wait between each announcement	15
jump	Extensions that are permitted to jump out of the agent group	41

Sample Syntax—Agent Group

```
type;alias;agents;gap_time;jump
acds;663;40 41 42;15;*
acds;664;40 41 42;15;40
```

Hunt Groups

The parameters for the hunt group are listed in Table A-3 (only *type* and *alias* are required).

Table A-3 Hunt Group Parameters

Parameter	Definition	Value
type	Account type	hunts
alias	Extension number of the hunt group account	74
display	Display name for the hunt group	hunt_74
st1_ext	Extensions that will be part of stage 1	40 41
st1_dur	Number of seconds the system should ring stage 1	10
st2_ext	Extensions that will be part of stage 2	43 45
st2_dur	Number of seconds the system should ring stage 2	15
st3_ext	(for unwanted stages, leave empty)	
st3_dur		
st4_ext	Extension or phone number for the final stage	70

Sample Syntax—Hunt Group

```
type;alias;display;st1_ext;st1_dur;st2_ext;st2_dur;st3_
ext;st3_dur;st4_ext
hunts;74;hunt_74;40 41;10;42;15;43 45;10;70
hunts;75;hunt_75;40 41;10;42 43;15;45 46;10;70
```

Conference Account

The parameters for the conference account are listed in Table A-4 (only *type* and *alias* are required).

Table A-4 Conference Account Parameters

Parameter	Definition	Value
type	Account type	conferences
alias	Extension number of the account	76
name	Name the conference	conf_76
intro	Type of introduction to use when the user enters the conference	ask_name none
pin	Access code for the moderator	777777
upin	Access code for the user	888888

Sample Syntax—Agent Groups

```
type;alias;name;intro;pin;upin
conferences;76;conf_76;ask_name;777777;888888
conferences;77;conf_77;none;111112;222222
```

Paging

The parameters for paging are listed in Table A-5 (only *type* and *alias* are required).

Table A-5 Paging Account Parameters

Parameter	Definition	Value
type	Account type	hoots
alias	Extension number of the account	662
display	Display name for the paging account	page_662
ext	Corresponds to the **Destination** setting of the paging account (when using unicast mode, enter a group of extension numbers; when using multicast mode, enter an IP address).	40

Parameter	Definition	Value
perm	Extensions that are permitted to monitor the account	41 42 43
mode	Type of paging account	unicast multicast
record	Indicates whether pages will be recorded	true false

Sample Syntax—Paging Account

```
type;alias;display;ext;perm;mode;record
hoots;662;page_662;40;41 42 43;unicast;true
hoots;661;page_661;*;*;multicast;false
```

Service Flags

The parameters for service flags are listed in Table A-6 (only *type* and *alias* are required).

Table A-6 Service Flag Parameters

Parameter	Definition	Value
type	Account type	hoots
alias	Extension number of the account	658
display	Display name for the account	srv_658
mode	Determines whether this service flag will be automatic (clock) or manual (when clock is chosen, the system will automatically use the schedule that is specified below).	clock manual
sound		night

Parameter	Definition	Value
mon	When the `clock` mode is used, the auto attendant will route calls according to the schedule that is indicated here.	`9:00-12:00 13:00-17:00`
tue		`9:00-17:00`
wed		`9:00-12:00 1:00P-4:00P`
thur		`9:00-17:00`
fri		`9:00-17:00`
sat		
sun		
holiday	Indicates a holiday schedule (i.e., the days on which the schedule should not be activated)	`12/24 1/1`

Sample Synax—Service Flags

```
type;alias;display;mode;sound;mon;tue;wed;thur;fri;sat;sun;
holiday
srvflags;658;srv_658;clock;night;9:00-12:0
0 13:00-17:00;9:00-17:00;9:00-12:00 1:00P-
4:00P;9:00-17:00;9:00-17:00;;;12/24 1/1
srvflags;659;srv_659;manu
al;;9:00-12:00;9:00-17:00;9:00-12:00 3:00P-
5:00P;9:00-17:00;9:00-17:00;;;1/1 3/19
```

Converting an Excel File to CSV

Once you have become familiar with the parameters that can be used for a particular account, you can prepare the file for CSV conversion.

1. Open the file that contains your source data. In the example shown below, the source file is an Excel file.

CompanyAddresses.xls

	A	B	C	D	E	F	G	H
1	First Name	Last Name	Address	City	State	ZIP	Number	Speed Dial
2	Fred	Feuerstein	101 Pleasant Street	Boston	MA	02101	(978) 123-4567	
3	Carl	Clever	10 Elm Street	Andover	MA	01845	(978) 324-4334	*12
4	Bruno	Carlonna	10 Waterview Street	Venice	Rome		+011 39 0577 1234567	
5	Chris	Smith	127 South Chadwick	Bradford	MA	01830	(978) 373-1111	
6	Jeb	Mossar	129 Maple Avenue	New York	NY	00501	(978) 123-7777	*15
7	Pye	Smith	33 Center Place	Amherst	NY	14051	(212) 123-3456	*11
8	Dressar	Flowers	88 Pembroke Road	Newburyport	MA	01950	(202) 345-1234	*13
9	Charlie	Porche	15 Main Street	Haverhill	MA	01832	(978) 345-1111	*19

2. Review the contents of your file to determine which material does not conform to the specified parameters for a particular account type. As a reminder, the allowable parameters for the extension account are listed below:

```
type;alias;ani;password;web_pass;first_name;display_
name;mb_pin;email_address;mac
```

Note: Your file cannot contain columns that do not conform to these parameters. In the exercise sample shown in Step 1 above, columns C, D, E, and F contain nonconforming material and will not be needed for the CSV conversion.

In addition to removing data, you may also need to add data. For example, it is recommended that you add columns for data such as ANIs, passwords, PIN codes, and MAC addresses so that you will not have to manually enter this data later on. To simplify this process, you can assign identical passwords and PIN codes to each extension and have the users create unique numbers once their phones have been registered.

3. Delete the nonconforming columns (**Edit** > **Delete**). The material that remains must correlate with the allowable parameters, as shown below:

CompanyAddresses.xls

	A	B	C	D	E
1	First Name	Last Name			
2	Fred	Feuerstein			
3	Carl	Clever			
4	Bruno	Carlonna			
5	Chris	Smith			
6	Jeb	Mossar			
7	Pye	Smith			
8	Dressar	Flowers			
9	Charlie	Porche			

4. When creating a block of extensions using a CSV file, the `type` and `alias` fields are mandatory. To accommodate these parameters, add two additional columns to your file. (To add a column using Excel, place your cursor in the first column, then click **Insert** > **Columns**.)

CompanyAddresses.xls

	A	B	C	D
1	type	alias	First Name	Last Name
2			Fred	Feuerstein
3			Carl	Clever
4			Bruno	Carlonna
5			Chris	Smith
6			Jeb	Mossar
7			Pye	Smith
8			Dressar	Flowers
9			Charlie	Porche

5. To accommodate other new material you would like to include, such as passwords, PIN codes, and other information, add columns for this information as well. This will simplify the process later on.

CompanyAddresses.xls

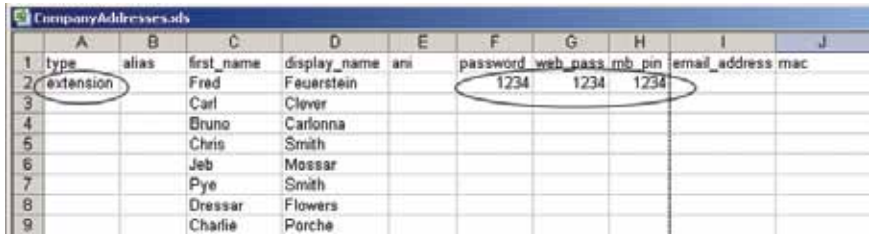
	A	B	C	D	E	F	G	H	I	J
1	type	alias	First Name	Last Name	ani	password	web_pass	mb_pin	email_address	mac
2			Fred	Feuerstein						
3			Carl	Clever						
4			Bruno	Carlonna						
5			Chris	Smith						
6			Jeb	Mossar						
7			Pye	Smith						
8			Dressar	Flowers						
9			Charlie	Porche						

6. Rename columns so that they conform to the extension parameters (Table A-1):

CompanyAddresses.xls

	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_name	ani	password	web_pass	mb_pin	email_address	mac
2			Fred	Feuerstein						
3			Carl	Clever						
4			Bruno	Carlonna						
5			Chris	Smith						
6			Jeb	Mossar						
7			Pye	Smith						
8			Dressar	Flowers						
9			Charlie	Porche						

7. Populate the empty fields. Begin by populating the fields that will have identical information, such as *`type`*, *`password`*, *`web_pass`*, and *`mb_pin`*. Type only the first entry as shown below:

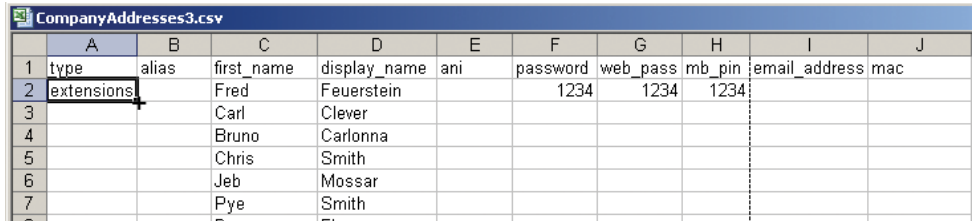


	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_name	ani	password	web_pass	mb_pin	email_address	mac
2	extension		Fred	Feuerstein		1234	1234	1234		
3			Carl	Clever						
4			Bruno	Carlonna						
5			Chris	Smith						
6			Jeb	Mossar						
7			Pye	Smith						
8			Dressar	Flowers						
9			Charlie	Porche						

These parameters are outlined as follows:

- *type*: When adding extensions, the value will always be `extensions`.
- *password*: This field can be populated with any type of password; however, the quickest method is to use the same password for all users and have the users change their own password.
- *web_pass*: See the previous comment.
- *mb_pin*: This field requires a PIN. The quickest method is to use the same password for all users and have the users change their own password.

8. To quickly populate the columns using Excel's Auto Fill feature, use the following instructions: Click on the cell containing the text you would like to repeat. (Extension numbers will be done later.) Place your cursor at the bottom-right corner until you see a plus sign. Then, holding down the **Alt** key, drag the plus sign down to the end of the column.



	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_name	ani	password	web_pass	mb_pin	email_address	mac
2	extensions		Fred	Feuerstein		1234	1234	1234		
3			Carl	Clever						
4			Bruno	Carlonna						
5			Chris	Smith						
6			Jeb	Mossar						
7			Pye	Smith						

9. Repeat Step 8 until the necessary columns have been populated.

CompanyAddresses3.csv

	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_name	ani	password	web_pass	mb_pin	email_address	mac
2	extensions		Fred	Feuerstein		1234	1234	1234		
3	extensions		Carl	Clever		1234	1234	1234		
4	extensions		Bruno	Carlonna		1234	1234	1234		
5	extensions		Chris	Smith		1234	1234	1234		
6	extensions		Jeb	Mossar		1234	1234	1234		
7	extensions		Pye	Smith		1234	1234	1234		
8	extensions		Dressar	Flowers		1234	1234	1234		
9	extensions		Charlie	Porche		1234	1234	1234		

Next, enter extensions for each account. Adding a block of extensions using Excel can be expedited using the Auto Fill tool, as explained below:

- Choose the extensions you that you will be using (make sure none of them are currently in use). For the example, in this exercise, extensions 509 through 516 will be used.
- Enter the first extension, as shown below:

CompanyAddresses3.csv

	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_na	ani	password	web_pass	mb_pin	email_addi	mac
2	extensions	509	Fred	Feuerstein		1234	1234	1234		
3	extensions		Carl	Clever		1234	1234	1234		
4	extensions		Bruno	Carlonna		1234	1234	1234		
5	extensions		Chris	Smith		1234	1234	1234		
6	extensions		Jeb	Mossar		1234	1234	1234		
7	extensions		Pye	Smith		1234	1234	1234		
8	extensions		Dressar	Flowers		1234	1234	1234		

- Click the bottom right-hand corner, then while holding down the **Ctrl** key, drag the double plus sign to the end of the column. The numbers will appear in sequential order, as shown below:

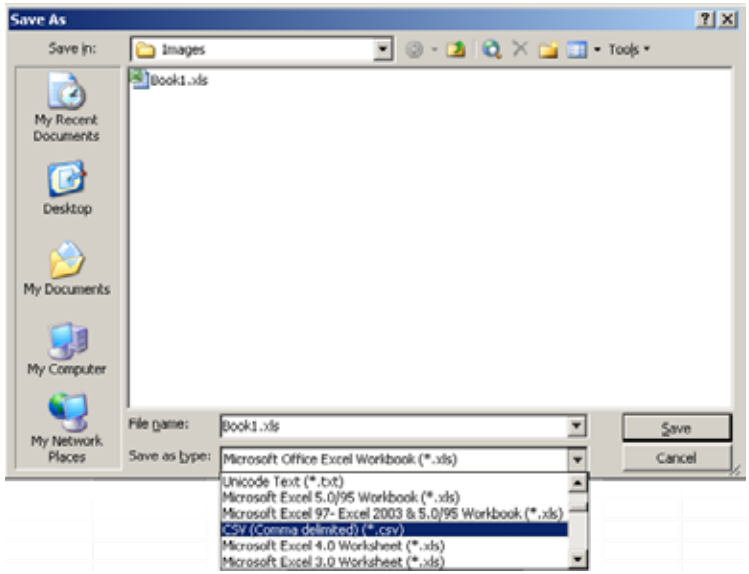
CompanyAddresses3.csv

	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_na	ani	password	web_pass	mb_pin	email_addi	mac
2	extensions	509	Fred	Feuerstein		1234	1234	1234		
3	extensions	510	Carl	Clever		1234	1234	1234		
4	extensions	511	Bruno	Carlonna		1234	1234	1234		
5	extensions	512	Chris	Smith		1234	1234	1234		
6	extensions	513	Jeb	Mossar		1234	1234	1234		
7	extensions	514	Pye	Smith		1234	1234	1234		
8	extensions	515	Dressar	Flowers		1234	1234	1234		
9	extensions	516	Charlie	Porche		1234	1234	1234		

10. Populate the remaining columns. These will need to be done manually:
    - *ani*:

- *email_address*: Supply the user with an email address.
- *mac*: Enter the MAC address of the phone that will be assigned to this extension.

11. Once you are satisfied with the contents of the file, save the file as a CSV file type (**File** > **Save As**).



12. Click **OK** when the following message appears:

Microsoft Excel
The selected file type does not support workbooks that contain multiple sheets.
• To save only the active sheet, click OK.
• To save all sheets, save them individually using a different file name for each, or choose a file type that supports multiple sheets.
OK
Cancel

13. Click **Yes** at the following message:

Microsoft Excel
Book1.csv may contain features that are not compatible with CSV (Comma delimited). Do you want to keep the workbook in this format?
• To keep this format, which leaves out any incompatible features, click Yes.
• To preserve the features, click No. Then save a copy in the latest Excel format.
• To see what might be lost, click Help.
Yes
No
Help

14. You now have a CSV file (the file name is at the top left-hand corner). Proceed to the next section to ensure that the integrity of the file has not been compromised in the conversion process.

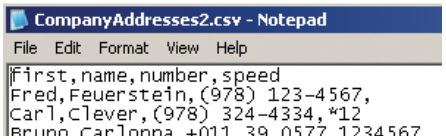
CompanyAddresses3.csv

	A	B	C	D	E	F	G	H	I	J
1	type	alias	first_name	display_na	ani	password	web_pass	mb_pin	email_addr	mac
2	extensions	509	Fred	Feuerstein		1234	1234	1234		
3	extensions	510	Carl	Clever		1234	1234	1234		
4	extensions	511	Bruno	Carlonna		1234	1234	1234		
5	extensions	512	Chris	Smith		1234	1234	1234		
6	extensions	513	Jeb	Mossar		1234	1234	1234		
7	extensions	514	Pye	Smith		1234	1234	1234		

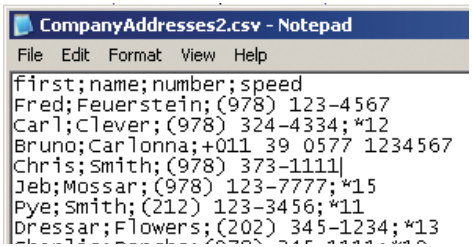
Changing the Field Separator and Validating the File

Now that the CSV has been created, you will need to go into the file to change the field separator from the default comma to a semicolon. You will also need to ensure that the integrity of the data has not been compromised. This includes checking for extra commas, extra quotation marks, and any other formatting which Excel may have inserted. This will be done from a plain text editor.

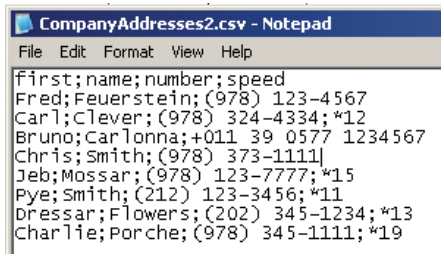
1. Open the new file from a plain-text program such as Notepad or TextEdit.



2. Check to make sure there are no extra commas other than between fields. Check also for extra quotation marks or other formatting which Excel may have inserted. In the CSV file shown above, Excel has inserted commas at the end of a few of the rows. Those will need to be deleted.
3. Change the comma to a semicolon by clicking **Edit** > **Replace**.



The final file is shown below. The file is now ready to be used for the address book upload.



4. To import the CSV file into snom ONE, see "Importing the CSV File" on page 498.

Creating a Domain Address Book

Address Book Parameters

When creating CSV files for a domain address book, be sure your data conforms to the structure of snom ONE's address book. Depending upon the particular file you will be converting to CSV, this may mean that you will need to remove information that does not conform to this layout. The acceptable parameters are listed in Table A-7.

Table A-7 Address Book Parameters

Parameter	Definition	Value
display number		
domain	Domain name (not required for single domains)	
first	Last name	Smith
name	First name	Fred

Parameter	Definition	Value
number	Phone number: The following characters are ignored by the system (although it is permissible to use these characters, they will not appear in the address book): - (hyphen) , (comma) (space) / (backslash) . (period) The plus (+) sign is permitted when entering global numbers, e.g., +49 (30) 386-12345.	`(978) 543 6545`
speed	Speed dial numbers cannot overlap with numbers that are in use as star codes (see Chapter 23 for the list of star codes).	`*12`
type	Black list/white list indicator: By default, all address book entries are classified as white list contacts. To specify that an entry should be placed on the black list, enter "black" into this field.	`black`
user		

Converting the Address Book to CSV

Once you have become familiar with the parameters that can be used for domain address books, you can prepare the file for CSV file conversion.

1. Open the source file. In the example shown below, the source file is an Excel file.

CompanyAddresses.xls

	A	B	C	D	E	F	G	H
1	First Name	Last Name	Address	City	State	ZIP	Number	Speed Dial
2	Fred	Feuerstein	101 Pleasant Street	Boston	MA	02101	(978) 123-4567	
3	Carl	Clever	10 Elm Street	Andover	MA	01845	(978) 324-4334	*12
4	Bruno	Carlonna	10 Waterview Street	Venice	Rome		+011 39 0577 1234567	
5	Chris	Smith	127 South Chadwick	Bradford	MA	01830	(978) 373-1111	
6	Jeb	Mossar	129 Maple Avenue	New York	NY	00501	(978) 123-7777	*15
7	Pye	Smith	33 Center Place	Amherst	NY	14051	(212) 123-3456	*11
8	Dressar	Flowers	88 Pembroke Road	Newburyport	MA	01950	(202) 345-1234	*13
9	Charlie	Porche	15 Main Street	Haverhill	MA	01832	(978) 345-1111	*19

2. Assess the contents of the file to determine which material does not conform to the parameters listed in Table A-7. As a reminder, the allowable parameters are listed below:

```
display_number;domain;first;name;number;speed;type
```

   Keep in mind that your file cannot contain columns that stray from these parameters. In the sample shown in Step 1, columns C, D, E, and F contain nonconforming material.

3. Delete the nonconforming columns (**Edit** > **Delete**). The material that remains must correlate with the allowable parameters, as shown below:

CompanyAddressesDeletedColumns.xls

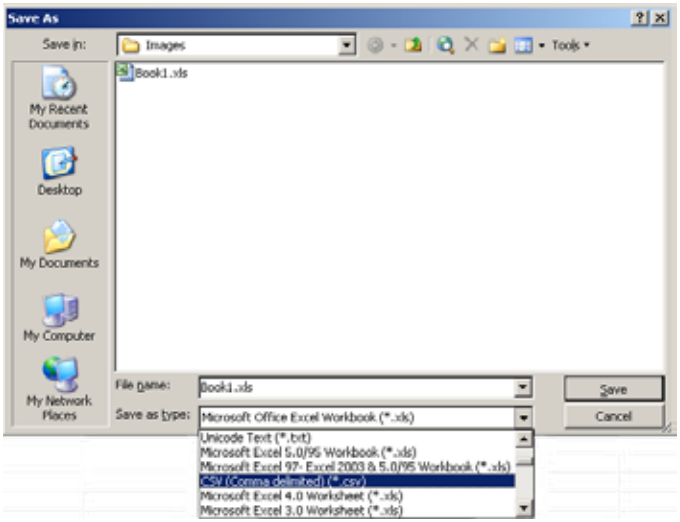
	A	B	C	D
1	First Name	Last Name	Number	Speed Dial
2	Fred	Feuerstein	(978) 123-4567	
3	Carl	Clever	(978) 324-4334	*12
4	Bruno	Carlonna	+011 39 0577 1234567	
5	Chris	Smith	(978) 373-1111	
6	Jeb	Mossar	(978) 123-7777	*15
7	Pye	Smith	(212) 123-3456	*11
8	Dressar	Flowers	(202) 345-1234	*13
9	Charlie	Porche	(978) 345-1111	*19

4. Change the first row to reflect the actual names of the parameters:

CompanyAddresses2.xls

	A	B	C	D
1	first	name	number	speed
2	Fred	Feuerstein	(978) 123-4567	
3	Carl	Clever	(978) 324-4334	*12
4	Bruno	Carlonna	+011 39 0577 1234567	
5	Chris	Smith	(978) 373-1111	
6	Jeb	Mossar	(978) 123-7777	*15
7	Pye	Smith	(212) 123-3456	*11
8	Dressar	Flowers	(202) 345-1234	*13
9	Charlie	Porche	(978) 345-1111	*19

5. If you would like to add another parameter, you could do so now. For this particular file, you could add the `type` parameter, so that white list contacts can be distinguished form black list contacts; however, there are so few black list contacts that this distinction could be made manually just as easily.
6. Once you are satisfied with the contents of the file, save the file as a CSV file type (**File** > **Save As**).



7. Click **OK** when the following message appears:

Microsoft Excel
The selected file type does not support workbooks that contain multiple sheets.
• To save only the active sheet, click OK.
• To save all sheets, save them individually using a different file name for each, or choose a file type that supports multiple sheets.
OK
Cancel

8. Click **Yes** at the following message:

Microsoft Excel
Book1.csv may contain features that are not compatible with CSV (Comma delimited). Do you want to keep the workbook in this format?
• To keep this format, which leaves out any incompatible features, click Yes.
• To preserve the features, click No. Then save a copy in the latest Excel format.
• To see what might be lost, click Help.
Yes
No
Help

9. You now have a CSV file, as is indicated by the file name in the top left-hand corner. Proceed to the next section to ensure that the integrity of the file has not been compromised in the conversion process.

CompanyAddresses2.csv

	A	B	C	D
1	first	name	number	speed
2	Fred	Feuerstein	(978) 123-4567	
3	Carl	Clever	(978) 324-4334	*12
4	Bruno	Carlonna	+011 39 0577 1234567	
5	Chris	Smith	(978) 373-1111	
6	Jeb	Mossar	(978) 123-7777	*15
7	Pye	Smith	(212) 123-3456	*11
8	Dressar	Flowers	(202) 345-1234	*13
9	Charlie	Porche	(978) 345-1111	*19

Changing the Field Separator and Validating the File

Now that the CSV has been created, you will need to go into the file to change the field separator from the default comma to a semicolon. You will also need to ensure that the integrity of the data has not been compromised. This includes checking for extra commas, extra quotation marks, and any other formatting which Excel may have inserted. This will be done from a plain text editor.

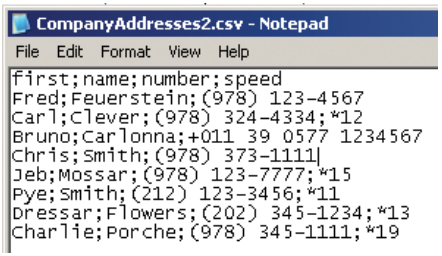
1. Open the new file from a plain-text reading program such as Notepad or TextEdit.

CompanyAddresses2.csv - Notepad

File Edit Format View Help

```
First,name,number,speed
Fred,Feuerstein,(978) 123-4567,
Carl,Clever,(978) 324-4334,*12
Bruno,Carlonna,+011 39 0577 1234567,
Chris,Smith,(978) 373-1111,
Jeb,Mossar,(978) 123-7777,*15
Pye,Smith,(212) 123-3456,*11
Dressar,Flowers,(202) 345-1234,*13
Charlie,Porche,(978) 345-1111,*19
```

2. Check to make sure there are no extra commas other than between fields. Check also for extra quotation marks or other formatting which Excel may have inserted. In the CSV file shown above, Excel has inserted commas at the end of a few of the rows. Those will need to be deleted.
3. Change the comma to a semicolon by clicking **Edit** > **Replace**. The final file is shown below. The file is now ready to be used for the address book upload.



4. To import the CSV file into snom ONE, proceed to the next section, "Importing the CSV File."

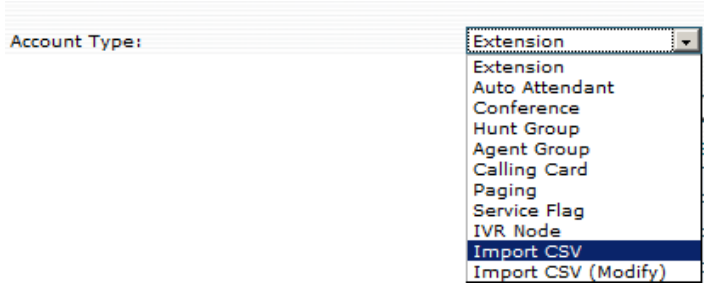
Importing the CSV File

Importing a CSV File for the Extension Account

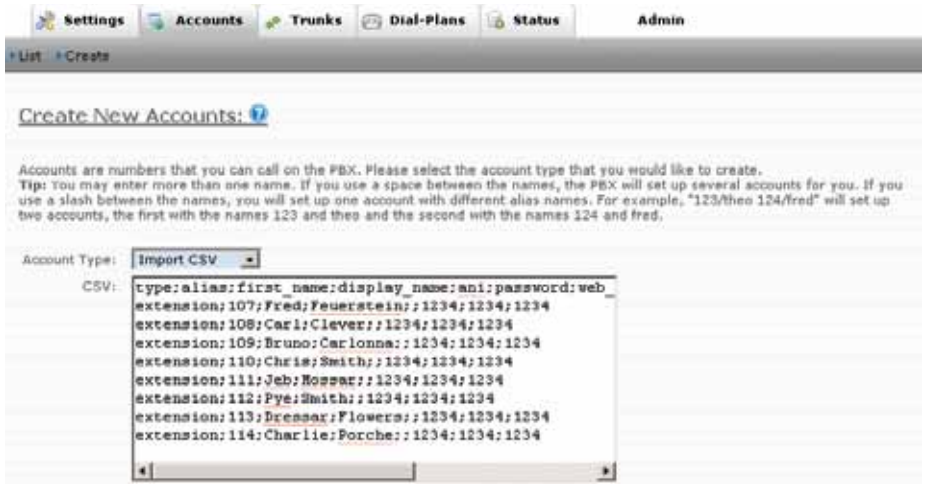
This section shows you how to import the CSV files for the extension account into snom ONE (the same procedure can be used for all account types).

1. Open the CSV file in a text editor (for example, Notepad).
2. Select the entire contents and copy it. (It will remain on your clipboard for a short time.)
3. Click **Accounts** within the domain, click **Create**.

4. From the dropdown list, choose **Import CSV**.



5. Paste the contents of the CSV file into the space provided:


Settings
Accounts
Trunks
Dial-Plans
Status
Admin
List
Create
Create New Accounts:
Accounts are numbers that you can call on the PBX. Please select the account type that you would like to create.
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up several accounts for you. If you use a slash between the names, you will set up one account with different alias names. For example, "123/theo 124/fred" will set up two accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
Import CSV
CSV:
type:alias:first_name:display_name:ani:password:web_
extension:107:Fred:Feuerstein:;1234:1234:1234
extension:108:Carl:Clever:;1234:1234:1234
extension:109:Bruno:Carlonna:;1234:1234:1234
extension:110:Chris:Smith:;1234:1234:1234
extension:111:Jeb:Rossar:;1234:1234:1234
extension:112:Pye:Smith:;1234:1234:1234
extension:113:Dresser:Flowers:;1234:1234:1234
extension:114:Charlie:Porche:;1234:1234:1234

6. Click **Create**.
7. To verify that the accounts were created, click **List** as shown below:

Settings
Accounts
Trunks
Dial-Plans
Status
Admin
List
Create
Create New Accounts:
Accounts are numbers that you can call on the PBX. Please select the account type that you would like to create.
Tip: You may enter more than one name. If you use a space between the names, the PBX will set up several accounts for you. If you use a slash between the names, you will set up one account with different alias names. For example, "123/theo 124/fred" will set up two accounts, the first with the names 123 and theo and the second with the names 124 and fred.
Account Type:
Extension
Dial Plan:
Domain Default
Plug and Play:
Manual

The extensions are listed with the other extensions of that domain.

509 Extension (Fred Feuerstein)
510 Extension (Carl Clever)
511 Extension (Bruno Carlonna)
512 Extension (Chris Smith)
513 Extension (Jeb Mossar)
514 Extension (Pye Smith)
515 Extension (Dressar Flowers)
516 Extension (Charlie Porche)

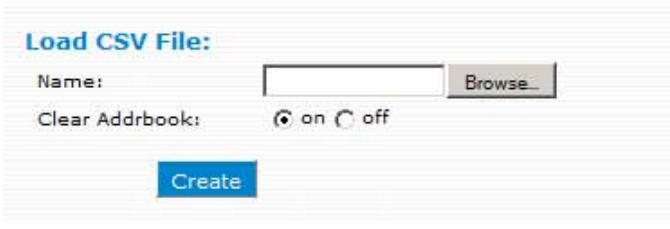
If you don't see the extensions, go to the troubleshooting section on page 501.

Importing CSV Files for Domain Address Books

This section explains how to import a CSV file that will be used as a domain address book. Use the following instructions from the snom ONE home page:

1. From the domain, click the **Settings** tab, then choose **Address-Book**:

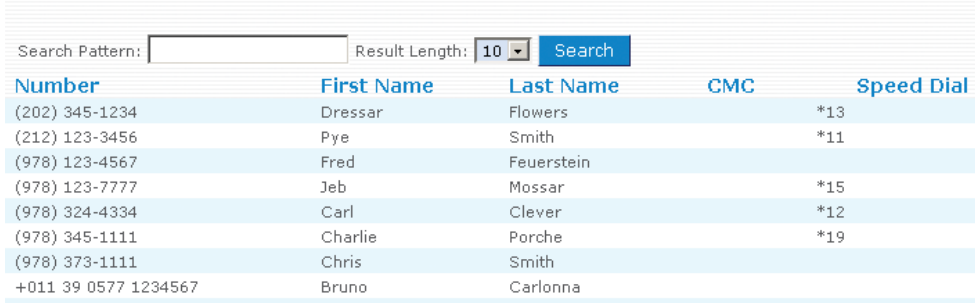
2. Scroll to the bottom of the page and click the Browse button.



3. Locate your CSV file and click **Open** to import it.

   Note: If you would like to retain any existing address book entries, set **Clear Addrbook** to **off**. Otherwise, the import will remove any previous entries.

4. Click **Create**. The new entries will be displayed in the address book.



Troubleshooting

Problem	Possible Cause(s)	Correction
Extensions do not appear.	Missing header	Be sure your CSV file contains a header row and that it includes the correct syntax (see page 480).
	Incorrect syntax.	Syntax must conform to the syntax shown in the parameter tables beginning on page 481.
Information appears in the wrong place (e.g., the first name appears in the web password field).	Too many tabs between fields.	Remove extra tabs from the CSV file.
After the CSV file was imported, the Accounts page reflects two entries for each extension.	Aliases will show up as extensions on the Accounts page, but internally, there will be only one extension. This is not a problem.	If you want to clean up the file, you can go back to defaults and take the space and the alias portion out of the CSV file and import it again. (Aliases will need to be entered manually using this method of CSV import.)

Appendix B

SIP OVERVIEW

SIP (Session Initiation Protocol) is a signaling protocol that is used to control multimedia communication sessions, such as voice and video calls, over Internet Protocol (IP). SIP is analogous to HTTP for voice and is essentially the glue that ties communications systems together, much like HTTP ties clients and servers together for worldwide communication. More and more vendors are implementing SIP as a standard telephony platform, and it is becoming increasingly popular. This appendix provides an introduction to SIP and is designed to introduce you to key concepts and mechanisms of the SIP protocol.

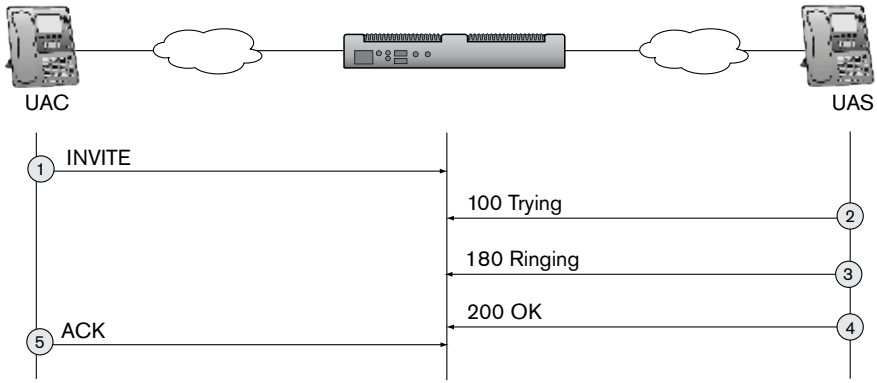
What is SIP?

Background

SIP was originally designed in 1996 to create a mechanism for inviting people to large-scale multipoint conferences on the Internet multicast backbone. The first version (SIP 2.0) was defined by RFC 2543, and by November of 2000, the protocol had been refined and clarified in RFC 3261. Though IP telephony didn't actually exist at the inception of RFC 3261, SIP evolved to provide a missing piece to the Internet architecture: A way for users to explicitly invite others users to join sessions over the Internet.

What is a SIP Session?

A SIP session is a related progression of events devoted to a particular activity occurring over the Internet. Activities can include two-way telephone calls, video conferencing, streaming multimedia distribution, instant messaging, presence, and online games.

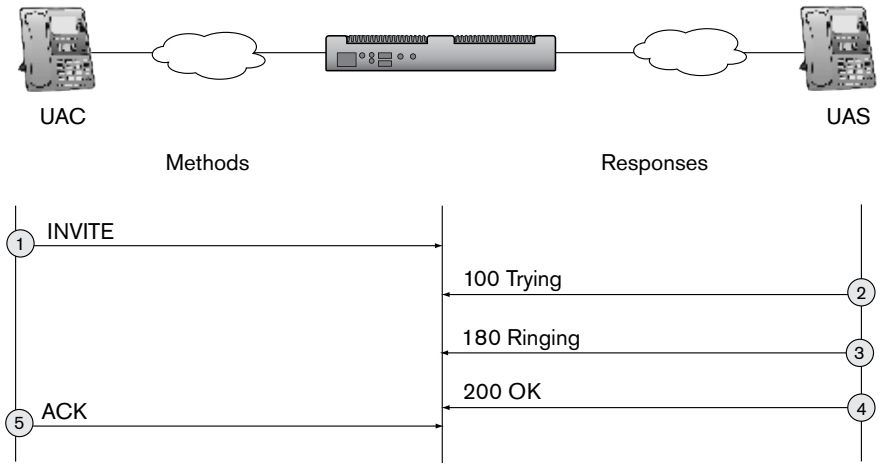


SIP knows nothing about the details of the sessions it controls. It only initiates, terminates, and modifies the sessions. Although SIP can work in a framework with other protocols— SOAP, HTTP, XML, VXML, WSDL, UDDI, and SDP—it does not perform any of their functions.

SIP Components

Entities interacting in a SIP scenario are known as User Agents (UAs), and there are two types of UAs: clients and servers.

- **User Agent Client (UAC)**: The UAC generates "methods" and sends them to servers (e.g., it sends an INVITE request and initiates a call).



- **User Agent Server (UAS):** The UAS receives the methods, processes them, and generates responses (e.g., it sends a 200 Ok response to indicate a successful session). The UAS may issue multiple responses to the UAC.

User Agent Clients

The UAC is often associated with the end user, since applications running on systems are used by people. The UAC can be any end-user device, such as a cell phone, multimedia handset, personal computer (PC), personal digital assistant (PDA), or a softphone.

The requests generated by the UAC are sent to a server (typically a proxy server) and are known as "methods," which will be discussed later.

Note: Non-IP devices like dumb phones can also be turned into SIP UAs by using an inexpensive analog telephone adapter (ATA) to make them SIP-aware. An ATA is a box with one or two analog ports with RJ11 jacks used for connecting regular analog phones to the VoIP network. Popular ones include the SIPura or Linksys PAP2.

User Agent Servers

Servers possess a predefined set of rules to handle the requests sent by clients and are usually part of the network. There are several types of servers:

Proxy Server— Proxy servers help track down addresses of recipients whose exact addresses are not known in advance. If the proxy server cannot find the address of the recipient, it will send the request to other proxy servers. Destinations include another extension on the same proxy server, the next-hop proxy server in the routing table, or a media server. SIP proxy servers use presence services to track users, which means users can be located regardless of their physical location. Proxy servers are the most common server in the SIP environment.

Registrar Server— A SIP registration server is responsible for registering devices. It does this by authenticating the device with a user name and password and keeping a table of IP addresses and extensions/phone numbers. This authentication process is similar to logging into a web server, which requires a user name and password. The registrations server makes it possible for users to alter the address at which they are contactable. Registrations play an important role in the process since SIP devices that

do not register cannot be called and SIP devices that do not successfully authenticate cannot make outbound calls. A media server is a device that handles any kind of media or RT, such as a voicemail server, a conference server, an IVR server, and a music on hold server.

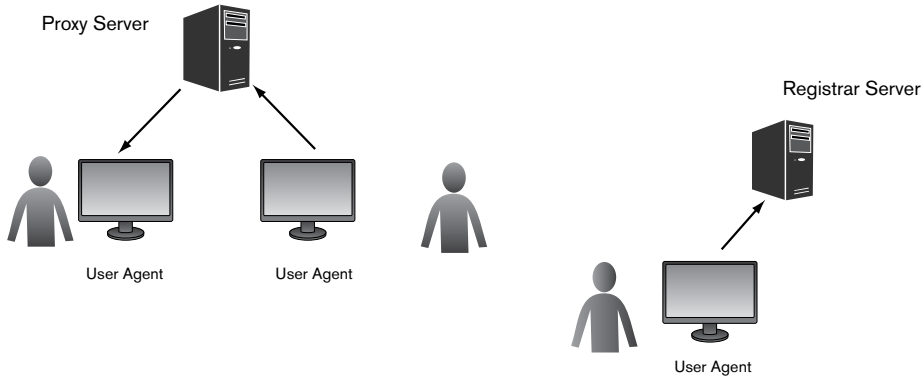


Figure B-1. Different Types of User Agent Servers (UASs)

Back-to-Back User Agent (B2BUA)

A B2BUA essentially bolts two user agents together in a back-to-back fashion, similar to two people standing back to back. A B2BAU establishes a two-legged call, keeping the SIP server in the middle of the call to orchestrate the details. One side of the session acts as the SIP UA server that receives the calls; the other side acts as the SIP UA client that establishes the other leg of the call. This "middle position" of the SIP server allows the system to execute difficult call scenarios, like recording a call, stepping out of the voicemail system (by pressing 0), barging into a call, and many other call scenarios that are very hard to do without this center position.

Figure B-2. Back-to-Back User Agent (B2BUA)

SIP Language

Similarities with HTML and SMTP

SIP shares some common characteristics with HTTP and SMTP. Like the latter two, SIP is an ASCII text-based protocol which makes it easy to read and troubleshoot. The text below is a SIP trace that shows a user inviting another use to a session.

Users are identified by a SIP address, known as a Uniform Resource Identifier (URI). A SIP URI is similar to an email address and is typically built around the user's phone number or host name (e.g., `sip:[your_number]@companyA.vonage.net`). This allows users to be redirected to another phone as easily as they would be redirected to another web page.

Types of Messages

SIP communication consists of two types of SIP messages—methods and responses. Methods are sent from the client to the server and are used to indicate the purpose of the request. The following six methods are part of RFC 3261.

Table B-1 RFC 3261 Methods

SIP Method	Description
INVITE	Establishes a session
ACK	Confirms an INVITE request
BYE	Ends a session
CANCEL	Cancels establishing of a session
REGISTER	Registers a user with a proxy/registrar
OPTIONS	Communicates information about the capabilities of the other side

Table B-2 Non-RFC 3261 Methods

SIP Method	Description	RFC
PRACK	Provisional acknowledgement	3262
SUBSCRIBE	Subscribes for an Event of Notification from the notifier	3265
NOTIFY	Notifies the subscriber of a new event	3265
PUBLISH	Publishes an event to the server	3903
INFO	Sends mid-session information that does not modify the session state	2976
REFER	Asks the recipient to issue a SIP request (call transfer)	3515
MESSAGE	Transports instant messages using SIP	3428
UPDATE	Modifies the state of a session without changing the state of the dialog	3311

Responses are sent from the server to the client and are used to indicate the status of the transaction. Responses are delivered in integer form (from 100 to 699) and are categorized as shown in Table B-3.

Table B-3 Categories of Response Codes

1xx	Informational responses
2xx	Success responses
3xx	Redirection responses
4xx	Request failures
5xx	Server errors
6xx	Global failures

Common response codes are shown below (for a complete list, see Table B-8).

Table B-4 Common Responses

Code	Definition	Occurrence
100	Trying	When the other side is trying to process the request
180	Ringing	When the other side is ringing
183	Session progress	
200	Ok	When the event is successful
302	Moved temporarily	When forwarding has been activated on the phone number that is being called
305	Use proxy	
400	Bad request	When a client enters a bad request
401	Unauthorized	When authentication is required
403	Forbidden	
404	Not found	When a phone number cannot be located
415	Unsupported media type	When the SDP contains no common codecs (this can happen if one side supports only G.729 and the PBX has no G.729 license defined)
500	Server internal error	When the SIP server is out of resources
501	Not implemented	
606	Not acceptable	When a global failure occurs (usually at the carrier level)

Content of Messages

SIP messages consist of the following three parts:

- **SIP URI:** The SIP URI is typically built around the user's phone number. This first line also indicates either the purpose of the request or the response given by the called party.

- **Message body:** SIP requests and responses can both contain message bodies. The content of the message body is usually a session description and contains syntax as shown in the message below.

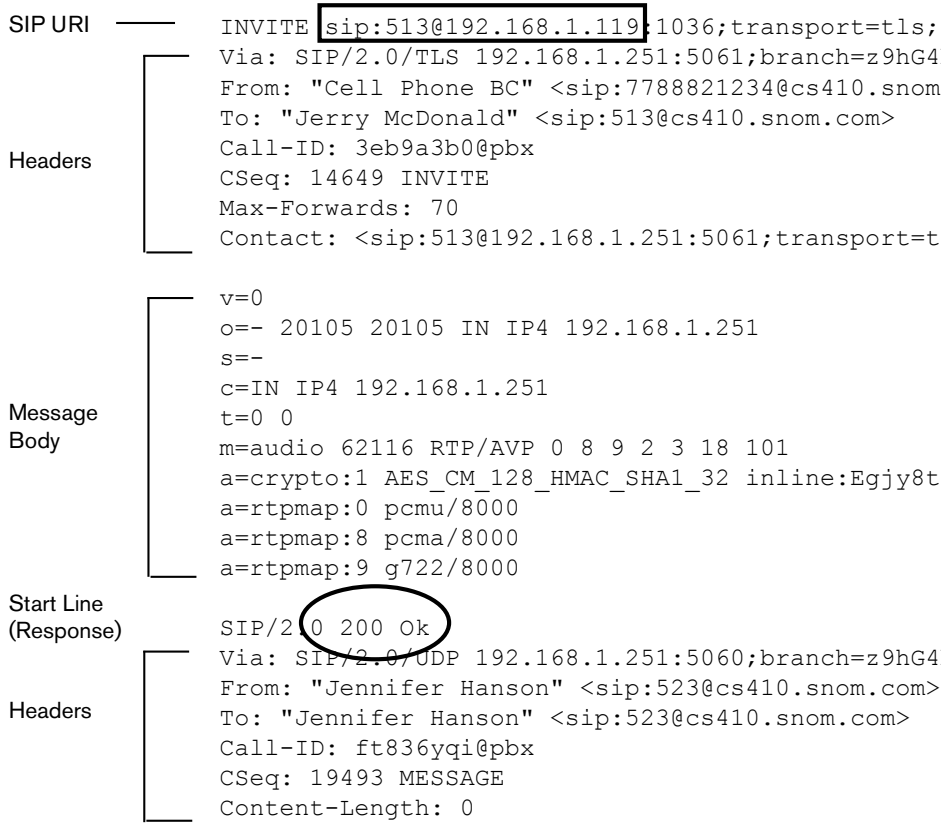


Figure B-3. Message Content

- **Headers:** SIP header fields provide additional information about the message. Common headers are shown below (for a complete list, see Table B-7).

Table B-5 Common SIP Headers

SIP Header	Description
`To`	Address of the called party or the destination party
`From`	Calling party or the caller-ID in some cases

SIP Header	Description
`Via`	Path taken by the request so far
`Call ID`	A unique number used to identify the call
`CSeq`	Used for keeping track of the conversation number
`Contact`	Used for identifying the user agent and the version of software used by the user agent

Describing the SIP Session

Besides methods and responses, SIP messages can also carry session descriptions in the form of Session Description Protocol (SDP). SDP is used for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. It includes information such as IP addresses, port numbers, and times and dates when the session is active. SDP session descriptions are text-based and consist of lines of text that are categorized as shown below (refer to Table B-6 for details on the syntax):

Session-level information

```
v=0
o=root 839347042 839347042 IN IP4 192.168.1.101
s=call
c=IN IP4 192.168.1.101
t=0 0
```

Media-level information

```
m=audio 52460 RTP/AVP 0 8 9 99 3 18 4 101
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:zw00j/jEiq68b1f
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=rtpmap:9 g722/8000
a=rtpmap:3 gsm/8000
a=rtpmap:18 g729/8000
a=fmtp:18 annexb=no
a=rtpmap:4 g723/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=rtcp-xr:voip-metrics stat-summary=loss,dup,jitt
a=sendrecv
```

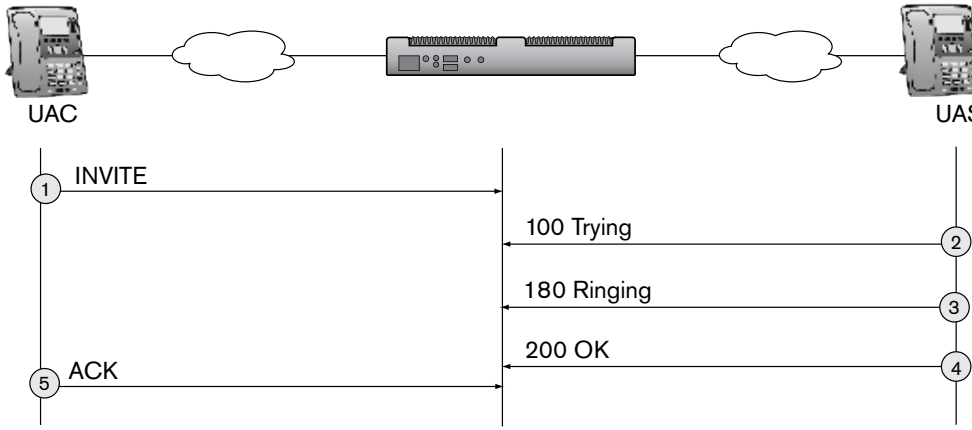
In the example shown above, the session-level section consists of five lines of text (always beginning with `v=0`, which indicates the version number of SDP), and the media-level section consists of one audio stream. The `a=rtpmap` lines convey information about the media format used.

Table B-6 Session Description Protocol (SDP) Syntax

Type	Description
`v`	Protocol version (optional)
`b`	Bandwidth information (optional)
`o`	Owner/creator and session identifier (optional)
`z`	Time zone adjustments
`s`	Session name (optional)
`k`	Encryption key (optional)
`i`	General information about the session (optional)
`a`	Session attribute (optional)
`u`	URI containing a description of the session (optional)
`t`	Time the session is active (optional)
`e`	Email address of the contact person (optional)
`r`	Times when the session will be repeated
`p`	Phone number to obtain information about the session (optional)
`m`	Media name and transport address
`c`	Connection information (not required if included in all media)
`i`	Information about a media line (optional)

SIP Call Process

Session Establishment



Call Flow

1. The UAC sends an INVITE message to `41@pbx.company.com` (UAS).
2. The UAS receives the request and responds with a 100 Trying.
3. The UAS sends a 180 Ringing response to the UAC when the phone begins ringing.
4. Once the call is picked up, the UAS send a 200 Ok message to the UAC.
5. The UAC sends an ACK request to confirm the 200 Ok response was received.

Note: The ACK method completes what is known as the three-way handshake—confirmation that a session has been successfully established. The INVITE is the only method where this occurs, and this is due to the large gap of time that often occurs between the INVITE itself and the 200 OK response (when a user can't find the phone, is running to the phone, etc.). So the ACK tells the called party that the caller hasn't hung up and has accepted the call.

```
INVITE sip:41@pbx.company.com;user=phone SIP/2.0
Via: SIP/2.0/TLS 192.168.0.32:2061;branch=z9hG4bK-
9gg3wzak;rport
From: "Roland Wright" <sip:40@pbx.company.com>;tag=g5ua0i7fz6
```

```
To: <sip:41@pbx.company.com;user=phone>
Call-ID: 3c2812339279-zvojwzvof6we
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:40@192.168.0.32:2061;transport=tls;line=i339wes
g>;reg-id=1
P-Key-Flags: resolution="31x13", keys="4"
User-Agent: snom360/7.3.14
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUB-
SCRIBE, PRACK, MESSAGE, INFO
Content-Length: 452
```

SIP/2.0 100 Trying

```
Via: SIP/2.0/TLS 192.168.0.32:2061;branch=z9hG4bK-
9gohvng3wzak;rport=2061
From: "Roland Wright" <sip:40@pbx.company.com>;tag=g5ua0i7fz6
To: <sip:41@pbx.company.com;user=phone>;tag=eed7a3b4e0
Call-ID: 3c2812339279-zvojwzvof6we
CSeq: 1 INVITE
Content-Length: 0
```

SIP/2.0 180 Ringing

```
Via: SIP/2.0/TLS 192.168.0.34:5061;branch=z9hG4bK-
e299f160c512cb066a3a536253aa4d44;rport=5061
From: "Roland Wright" <sip:40@pbx.company.com>;tag=1521860827
To: "Rachel Reed" <sip:41@pbx.company.com>;tag=ozac09qwnh
Call-ID: f6f17567@pbx
CSeq: 28592 INVITE
Contact: <sip:41@192.168.0.31:1037;transport=tls;line=zs4m8le
i>;reg-id=1
Require: 100rel
RSeq: 1
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, SUB-
SCRIBE, PRACK, MESSAGE, INFO
Allow-Events: talk, hold, refer, call-info
Content-Length: 0
```

```
[7] 2010/04/14 16:10:31:      SIP Rx tls:192.168.0.31:1037:
```

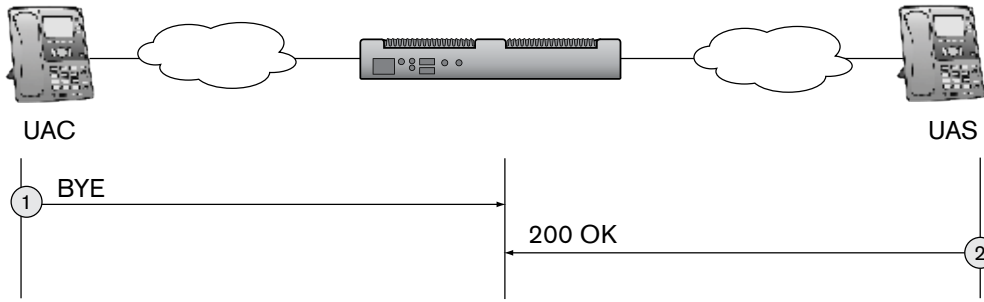
SIP/2.0 200 Ok

```
Via: SIP/2.0/TLS 192.168.0.34:5061;branch=z9hG4bK-
08d0f56ed1e8d82deb32779c5a2cc55b;rport=5061
```

```
From: "Roland Wright" <sip:40@pbx.company.com>;tag=1521860827
To: "Rachel Reed" <sip:41@pbx.company.com>;tag=ozac09qwnh
Call-ID: f6f17567@pbx
CSeq: 28593 PRACK
Contact: <sip:41@192.168.0.31:1037;transport=tls;line=zs4m8le
i>;reg-id=1
Content-Length: 0
```

```
ACK sip:41@192.168.0.31:1037;transport=tls;line=zs4m8lei
SIP/2.0
Via: SIP/2.0/TLS 192.168.0.34:5061;branch=z9hG4bK-
6dcf1018159b8e96b7b6d62a758d77fd;rport
From: "Roland Wright" <sip:40@pbx.company.com>;tag=1521860827
To: "Rachel Reed" <sip:41@pbx.company.com>;tag=ozac09qwnh
Call-ID: f6f17567@pbx
CSeq: 28592 ACK
Max-Forwards: 70
Contact: <sip:41@192.168.0.34:5061;transport=tls>
Content-Length: 0
```

Session Termination



Call Flow

1. Once the caller hangs up, a BYE is sent to the UAS.
2. The UAS receives the request and responds with a 200 Ok.

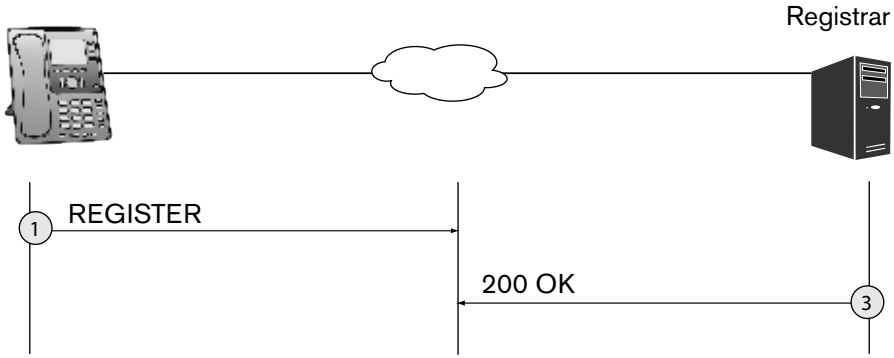
```
BYE sip:40@192.168.0.32:2061;transport=tls;line=i339wesg
SIP/2.0
```

```
Via: SIP/2.0/TLS 192.168.0.34:5061;branch=z9hG4bK-
eec7092e42e0694ecd8be3d3e9400816;rport
From: <sip:41@pbx.company.com;user=phone>;tag=eed7a3b4e0
To: "Roland Wright" <sip:40@pbx.company.com>;tag=g5ua0i7fz6
Call-ID: 3c2812339279-zvojwzvof6we
CSeq: 23626 BYE
Max-Forwards: 70
Contact: <sip:40@192.168.0.34:5061;transport=tls>
RTP-RxStat: Dur=20,Pkt=970,Oct=170720,Underun=0
RTP-TxStat: Dur=18,Pkt=975,Oct=171600
Content-Length: 0
[7] 2010/04/14 16:10:50:      SIP Rx tls:192.168.0.32:2061:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 192.168.0.34:5061;branch=z9hG4bK-
eec7092e42e0694ecd8be3d3e9400816;rport=5061
From: <sip:41@pbx.company.com;user=phone>;tag=eed7a3b4e0
To: "Roland Wright" <sip:40@pbx.company.com>;tag=g5ua0i7fz6
Call-ID: 3c2812339279-zvojwzvof6we
CSeq: 23626 BYE
Contact: <sip:40@192.168.0.32:2061;transport=tls;line=i339wes
g>;reg-id=1
User-Agent: snom360/7.3.14
RTP-RxStat: Total_Rx_Pkts=976,Rx_Pkts=972,Rx_Pkts_
Lost=0,Remote_Rx_Pkts_Lost=0
RTP-TxStat: Total_Tx_Pkts=974,Tx_Pkts=974,Remote_Tx_Pkts=751
Content-Length: 0
```

REGISTER Request

The `Contact` field is used by the SIP UA when using the REGISTER method. Once it receives the IP and configuration from the registrar, the SIP UA can begin registering (scenario 1 shown below). If the UA is challenged for authenication, it will resend the registration request with the necessary credentials (realm, username, password), if it has been set in the server. A 200 OK acknowledges a successful registration (scenario 2 on page 518).

Scenario 1



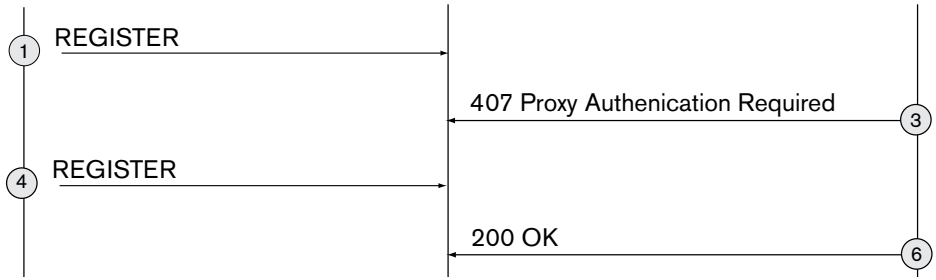
Call Flow

1. The UAC tries to register the user's SIP address.
2. The address is located, so a 200 OK response is sent to the UAC.

Scenario 1

```
REGISTER sip:cs410.snom.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.103:2077;branch=z9hG4bK-
rib4emgq;rport
From: "Hanna Flanders" <sip:520@cs410.snom.
com>;tag=fwxg2s0u4i
To: "Hanna Flanders" <sip:520@cs410.snom.com>
Call-ID: 3c267028e8ad-q7dwiql86rvc
CSeq: 6134 REGISTER
Max-Forwards: 70
Contact: <sip:520@192.168.1.103:2077;transport=tls;line=ibey
jpgk>;reg-id=1;q=1.0;+sip.instance="<urn:uuid:0fe6493a-4223-
49f7-9aa6-4fb5e5198e0f>"
[7] 2010/04/14 16:05:16:      SIP Tx tls:192.168.1.103:2077:
SIP/2.0 200 Ok
```

Scenario 2



Call Flow

1. The UAC tries to register the user's SIP address. The Web server (running the Web site) thinks that the HTTP data stream sent from the UAC was correct, but access to the URL resource requires the prior use of a proxy server that needs some authentication which has not been provided, so it responds with a 407 Proxy Authentication Required response.
2. The user logs in (enters user ID and password) with the proxy server. The UAC resends the REGISTER method.
3. The UAS responds with a 200 OK.

Scenario 2

```
REGISTER sip:itsp.com SIP/2.0
Via: SIP/2.0/UDP 75.150.83.2:5060;branch=z9hG4bK-
79d064228874f311c131a824e14e910f;rport
From: "itsp" <sip:17772830314@itsp.com>;tag=45682
To: "itsp" <sip:17772830314@itsp.com>
Call-ID: niyrncl8@pbx
CSeq: 8042 REGISTER
Max-Forwards: 70
Contact: <sip:17772830314@75.150.83.2:5060;transport=udp;line
=19ca14e7>;+sip.instance="<urn:uuid:7e96105b-8c8b-440e-a0aa-
07add8c80727>"

SIP/2.0 407 Proxy Authentication Required
v: SIP/2.0/UDP 75.150.83.2:5060;branch=z9hG4bK-
79d064228874f311c131a824e14e910f;rport=5060
```

```
f: "itsp" <sip:17772830314@itsp.com>;tag=45682
t: "itsp" <sip:17772830314@itsp.com>
i: niyrncl8@pbx
CSeq: 8042 REGISTER
Proxy-Authenticate: Digest realm="itsp.com",
domain="sip:itsp.com", nonce="ab45353d389d01ba208623
2c09417752", opaque="", stale=TRUE, algorithm=MD5
l: 0
```

```
[7] 2010/04/14 16:05:17:      SIP Tx udp:204.11.192.31:5080:
REGISTER sip:itsp.com SIP/2.0
Via: SIP/2.0/UDP 75.150.83.2:5060;branch=z9hG4bK-
a071e61e35d725f2c9a17c9bf2edb7f7;rport
From: "itsp" <sip:17772830314@itsp.com>;tag=45682
To: "itsp" <sip:17772830314@itsp.com>
Call-ID: niyrncl8@pbx
CSeq: 8043 REGISTER
Max-Forwards: 70
Contact: <sip:17772830314@75.150.83.2:5060;transport=udp;line
=19ca14e7>;+sip.instance="<urn:uuid:7e96105b-8c8b-440e-a0aa-
07add8c80727>"
User-Agent: snom-PBX/4.0.1.3453
Supported: outbound
Proxy-Authorization: Digest realm="itsp.com",nonce="ab45
353d389d01ba2086232c09417752",response="664617e317a5c34
448f276db3932be2f",username="17772830314",uri="sip:itsp.
com",algorithm=MD5
Expires: 3600
Content-Length: 0
```

```
SIP/2.0 200 Ok
```

CANCEL Request

The CANCEL request cancels pending transactions and generates an error response to the pending request. CANCEL has no effect on requests that have already received a final response (e.g., an ACK). Therefore, the CANCEL method is often associated with methods that require lengthy response times, such as the INVITE. A UAS that receives a CANCEL request for an INVITE but hasn't yet sent a final response would

cease ringing and then respond to the INVITE with a specific error response (a 487, as shown below).

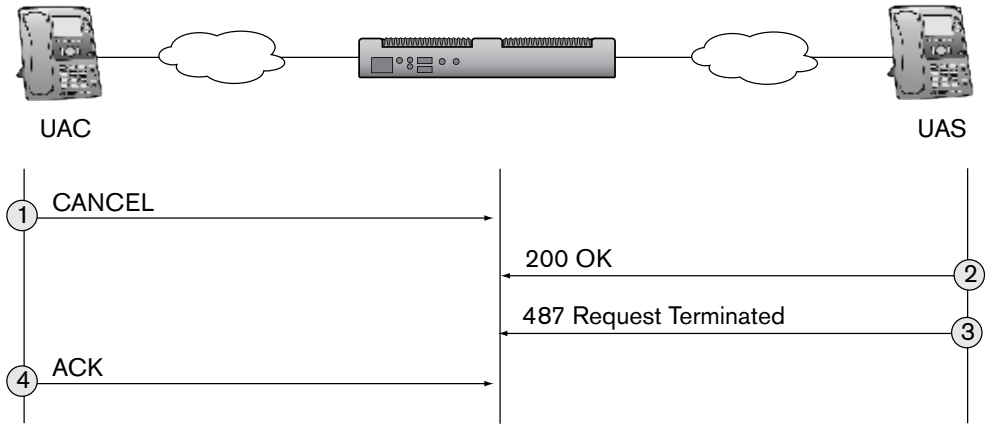


Figure B-4. CANCEL Request—INVITE Response 487 Request Terminated

Call Flow

1. A user makes a call, but after a few rings decides to hang up, so a CANCEL request for the previous INVITE is sent by the client to the server.
2. The called party's phone stops ringing, and a 200 OK response for the CANCEL is sent by the server to the client. The server then sends back a 487 Transaction Terminated response.
3. The client acknowledges the response by sending an ACK.

```
CANCEL sip:50@localhost;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.0.32:2048;branch=z9hG4bK-
lg7xoa360cuh;rport
From: "PC PBX 51" <sip:51@localhost>;tag=u58kfgll03
To: <sip:50@localhost;user=phone>
Call-ID: 3c2c575f0429-38s24k0wrdrx
CSeq: 2 CANCEL
Max-Forwards: 70
Reason: SIP;cause=487;text="Request terminated by user"
Content-Length: 0
```

```
[7] 2010/04/28 11:21:27:      SIP Tx udp:192.168.0.32:2048:
SIP/2.0 200 Ok
Via: SIP/2.0/UDP 192.168.0.32:2048;branch=z9hG4bK-
lg7xoa360cuh;rport=2048
From: "PC PBX 51" <sip:51@localhost>;tag=u58kfgll03
To: <sip:50@localhost;user=phone>;tag=4de5095638
Call-ID: 3c2c575f0429-38s24k0wrdrx
CSeq: 2 CANCEL
Contact: <sip:51@192.168.0.33:5060>
User-Agent: snom-PBX/4.0.1.3475
Content-Length: 0

[7] 2010/04/28 11:21:27:      SIP Tx udp:192.168.0.32:2048:
SIP/2.0 487 Request Terminated
Via: SIP/2.0/UDP 192.168.0.32:2048;branch=z9hG4bK-
lg7xoa360cuh;rport=2048
From: "PC PBX 51" <sip:51@localhost>;tag=u58kfgll03
To: <sip:50@localhost;user=phone>;tag=4de5095638
Call-ID: 3c2c575f0429-38s24k0wrdrx
CSeq: 2 INVITE
Contact: <sip:51@192.168.0.33:5060>
Supported: 100rel, replaces, norefersub
Allow-Events: refer
Allow: INVITE, ACK, CANCEL, BYE, REFER, PRACK, INFO, UPDATE
Accept: application/sdp
User-Agent: snom-PBX/4.0.1.3475
Content-Length: 0

[7] 2010/04/28 11:21:27:      SIP Tx udp:192.168.0.31:1024:
CANCEL sip:50@192.168.0.31:1025;line=npbudr1b SIP/2.0
Via: SIP/2.0/UDP 192.168.0.33:5060;branch=z9hG4bK-
9611418f8bbb34f24b5482fb86159ddd;rport
From: "Fifty One" <sip:51@pbx.company.com>;tag=33392
To: "Robyn Wright" <sip:50@pbx.company.com>
Call-ID: a8c5d213@pbx
CSeq: 21261 CANCEL
Max-Forwards: 70
Content-Length: 0

[7] 2010/04/28 11:21:27:      SIP Rx udp:192.168.0.31:1024:
```

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.0.33:5060;branch=z9hG4bK-
9611418f8bbb34f24b5482fb86159ddd;rport=5060
From: "Fifty One" <sip:51@pbx.company.com>;tag=33392
To: "Robyn Wright" <sip:50@pbx.company.com>;tag=55ay4g1375
Call-ID: a8c5d213@pbx
CSeq: 21261 CANCEL
Content-Length: 0

[7] 2010/04/28 11:21:27:      Call a8c5d213@pbx#33392: Clear
last request
[7] 2010/04/28 11:21:27:      SIP Rx udp:192.168.0.31:1024:
SIP/2.0 487 Request Terminated
Via: SIP/2.0/UDP 192.168.0.33:5060;branch=z9hG4bK-
9611418f8bbb34f24b5482fb86159ddd;rport=5060
From: "Fifty One" <sip:51@pbx.company.com>;tag=33392
To: "Robyn Wright" <sip:50@pbx.company.com>;tag=55ay4g1375
Call-ID: a8c5d213@pbx
CSeq: 21261 INVITE
Contact: <sip:50@192.168.0.31:1025;line=npbudr1b>;reg-id=1
Content-Length: 0

[7] 2010/04/28 11:21:27: Call a8c5d213@pbx#33392: Clear last
INVITE
[7] 2010/04/28 11:21:27:      SIP Tx udp:192.168.0.31:1024:
ACK sip:50@192.168.0.31:1025;line=npbudr1b SIP/2.0
Via: SIP/2.0/UDP 192.168.0.33:5060;branch=z9hG4bK-
9611418f8bbb34f24b5482fb86159ddd;rport
From: "Fifty One" <sip:51@pbx.company.com>;tag=33392
To: "Robyn Wright" <sip:50@pbx.company.com>;tag=55ay4g1375
Call-ID: a8c5d213@pbx
CSeq: 21261 ACK
Max-Forwards: 70
Contact: <sip:50@192.168.0.33:5060;transport=udp>
Content-Length: 0

[5] 2010/04/28 11:21:27:      INVITE Response 487 Request
Terminated: Terminate a8c5d213@pbx
[7] 2010/04/28 11:21:27:      SIP Rx udp:192.168.0.32:2048:
ACK sip:50@localhost;user=phone SIP/2.0
```

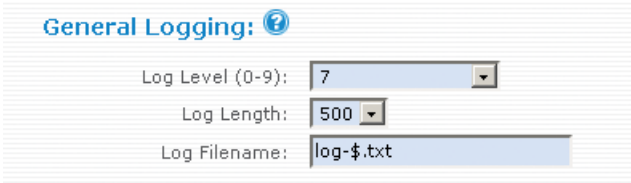
```
Via: SIP/2.0/UDP 192.168.0.32:2048;branch=z9hG4bK-
lg7xoa360cuh;rport
From: "PC PBX 51" <sip:51@localhost>;tag=u58kfgll03
To: <sip:50@localhost;user=phone>;tag=4de5095638
Call-ID: 3c2c575f0429-38s24k0wrdrx
CSeq: 2 ACK
Max-Forwards: 70
Contact: <sip:51@192.168.0.32:2048;line=o4a1zo97>;reg-id=1
Content-Length: 0
```

snom ONE Settings and SIP Traces

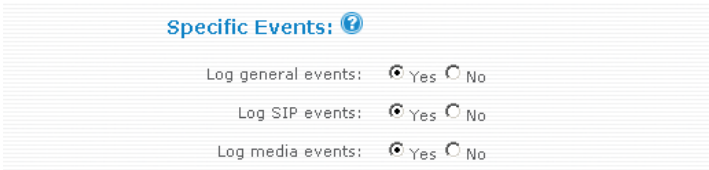
Viewing SIP Traces

This section shows you how to turn SIP logging on and view SIP traces.

1. Navigate to **Admin** > **Settings** > **Logging**.
2. Under **General Logging**, set the log level to 7.



3. Under **Specific Events**, set **Log SIP Events** to **yes**.



4. Click **Save**.
5. To view the SIP trace, navigate to **Status** > **Call Log**.

Logfile Syntax

Figure B-6 shows a sample logfile and the syntax that typically appears in one.

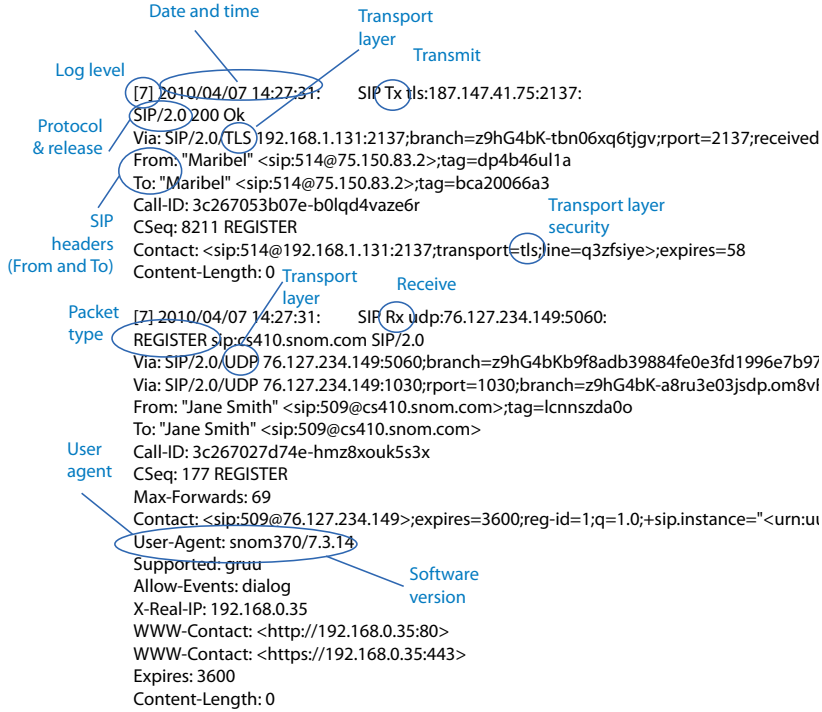


Figure B-5. Sample Logfile

Troubleshooting with Logfiles

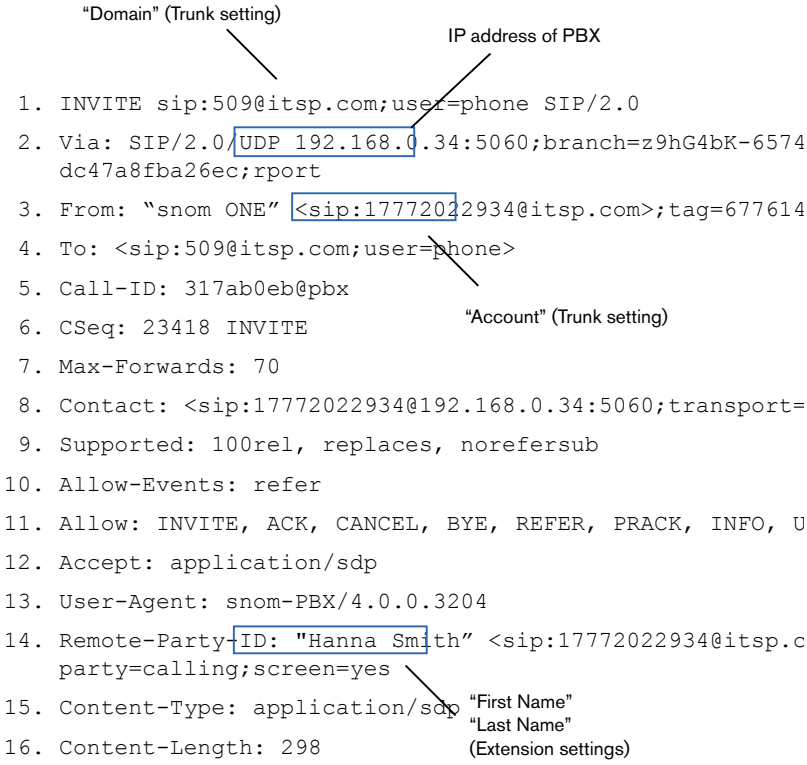
The logfile can be used to troubleshoot network issues. When seeking assistance outside your network, SIP traces can be especially helpful.

1. Click **Clear** to clear the log if necessary.
2. Make a phone call.
3. Click **Reload**, then navigate to **Status** > **Call Log**.

The SIP trace can be pasted into an email or a text editor and used for troubleshooting.

Trunk and Extension Settings

Settings made from the web interface (see Figure B-6 on next page) will affect what is in the SIP INVITE.



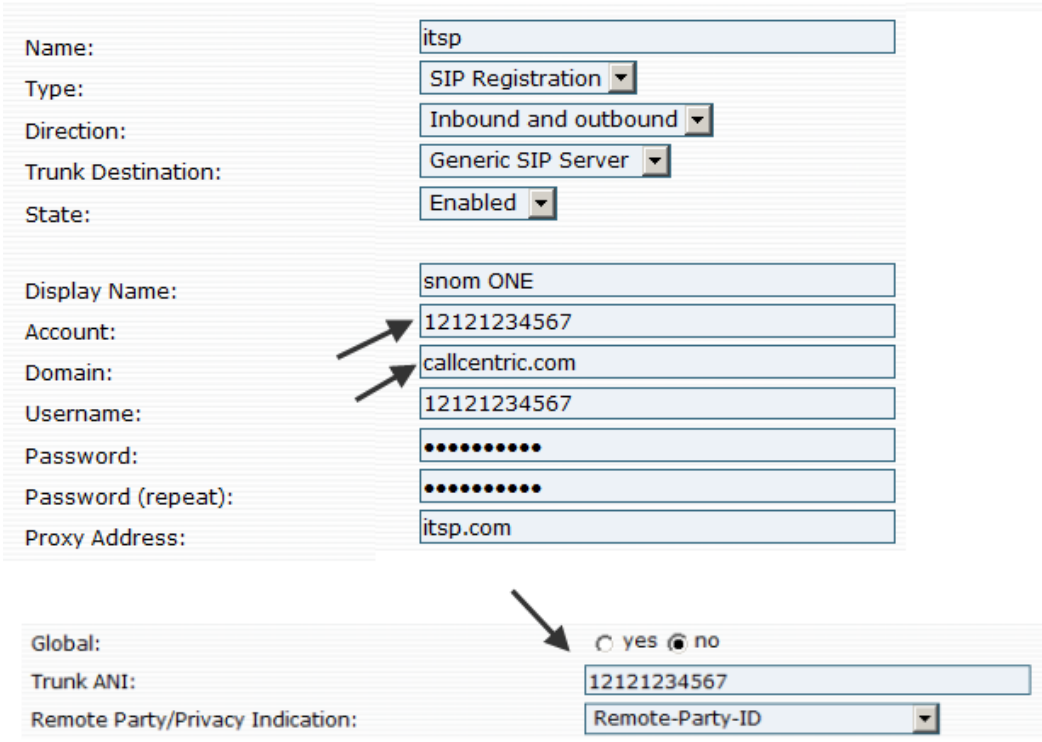


Figure B-6. Trunk Settings

Supporting Tables

Table B-7 SIP Headers

Header	Abbrev.	Header	Abbrev.
Accept		Organization	
Accept-Contact	a	P-Access-Network-Info	
Accept-Encoding		P-Answer-State	
Accept-Language		P-Asserted-Identity	
Accept-Resource-Priority		P-Associated-URI	
Alert-Info		P-Called-Party-ID	

Header	Abbrev.	Header	Abbrev.
Allow		P-Charging-Function-Addresses	
Allow-Events	u	P-Charging-Vector	
Answer-Mode		P-DCS-Billing-Info	
Authentication-Info		P-DCS-LAES	
Authorization		P-DCS-OSPS	
Call-ID	i	P-DCS-Redirect	
Call-Info		P-DCS-Trace-Party-ID	
Contact	m	P-Early-Media	
Content-Disposition		P-Media-Authorization	
Content-Encoding	e	P-Preferred-Identity	
Content-Language		P-Profile-Key	
Content-Length	l	P-Refused-URI-List	
Content-Type	c	P-Served-User	
CSeq		P-User-Database	
Date		P-Visited-Network-ID	
Encryption	Dep.*	Path	
Error-Info		Permission-Missing	
Event	o	Priority	
Expires		Priv-Answer-Mode	
Flow-Timer		Privacy	
From	f	Proxy-Authenticate	
Hide	Dep.*	Proxy-Authorization	
History-Info		Proxy-Require	
Identity	y	RAck	
Identity-Info	n	Reason	
In-Reply-To		Record-Route	
Join		Refer-Sub	
Max-Forwards		Referred-By	
MIME-Version		Replaces	

Header	Abbrev.	Header	Abbrev.
Min-Expires		Resource-Priority	
Min-SE		Response-Key	Dep.*
Retry-After		Target-Dialog	
Route		Timestamp	
RSeq		To	t
Security-Client		Trigger-Consent	
		Unsupported	
SIP-If-Match		User-Agent	
Subject	s	Via	v
Subscription-State		Warning	
Supported	k	WWW-Authenticate	
Suppress-If-Match			

* These headers have been deprecated.

Table B-8 SIP Response Codes

1xx—Informational Responses		423	Interval Too Brief
100	Trying	424	Bad Location Information
180	Ringing	428	Use Identity Header
181	Call Is Being Forwarded	429	Provide Referrer Identity
182	Queued	433	Anonymity Disallowed
183	Session Progress	436	Bad Identity-Info
2xx—Successful Responses		437	Unsupported Certificate
200	OK	438	Invalid Identity Header
202	Accepted	480	Temporarily Unavailable
3xx—Redirection Responses		481	Call/Transaction Does Not Exist
300	Multiple Choices	482	Loop Detected
301	Moved Permanently	483	Too Many Hops
302	Moved Temporarily	484	Address Incomplete
305	Use Proxy	485	Ambiguous

380	Alternative Service	486	Busy Here
4xx—Client Failure Responses		487	Request Terminated
400	Bad Request	488	Not Acceptable Here
401	Unauthorized	489	Bad Event
402	Payment Required	491	Request Pending
403	Forbidden	493	Undecipherable
404	Not Found (User not found)	494	Security Agreement Required
405	Method Not Allowed	5xx—Server Failure Responses	
406	Not Acceptable	500	Server Internal Error
407	Proxy Authentication Required	501	Not Implemented
408	Request Timeout	502	Bad Gateway
409	Conflict	503	Service Unavailable
410	Gone	504	Server Time-out
412	Conditional Request Failed	505	Version Not Supported
413	Request Entity Too Large	513	Message Too Large
414	Request-URI Too Long	580	Precondition Failure
415	Unsupported Media Type	6xx—Global Failure Responses	
416	Unsupported URI Scheme	600	Busy Everywhere
417	Unknown Resource-Priority	603	Decline
420	Bad Extension	604	Does Not Exist Anywhere
421	Extension Required	606	Not Acceptable
422	Session Interval Too Small		

Appendix C

SNOM ONE AND EXCHANGE

This appendix shows you how to set up Microsoft Exchange 2007/2010 UM with your snom ONE software. Although this setup provides basic functionality to get you started, keep in mind that both Exchange 2007/2010 UM and snom ONE can be customized extensively, which allows for more complex configurations than what is shown here. The configuration resembles the setup of the Microsoft Speech Server, as we suspect the underlying engines are alike.

When using snom ONE with Exchange, you can redirect calls, voicemail, and email to the mailbox of the Exchange server. You can also use the calendar and the address book. Exchange's address book allows you to initiate outbound calls and perform voice-activated dialing for internal or external calls. Exchange's auto attendant allows you to use your voice to call extensions.

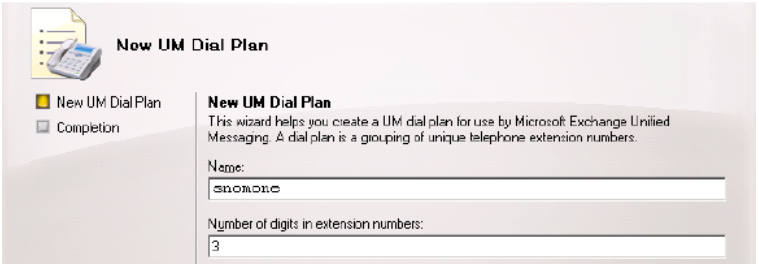
Note: Exchange does not send an MWI (message waiting indication) when a new message has arrived.

Configuring Exchange for snom ONE

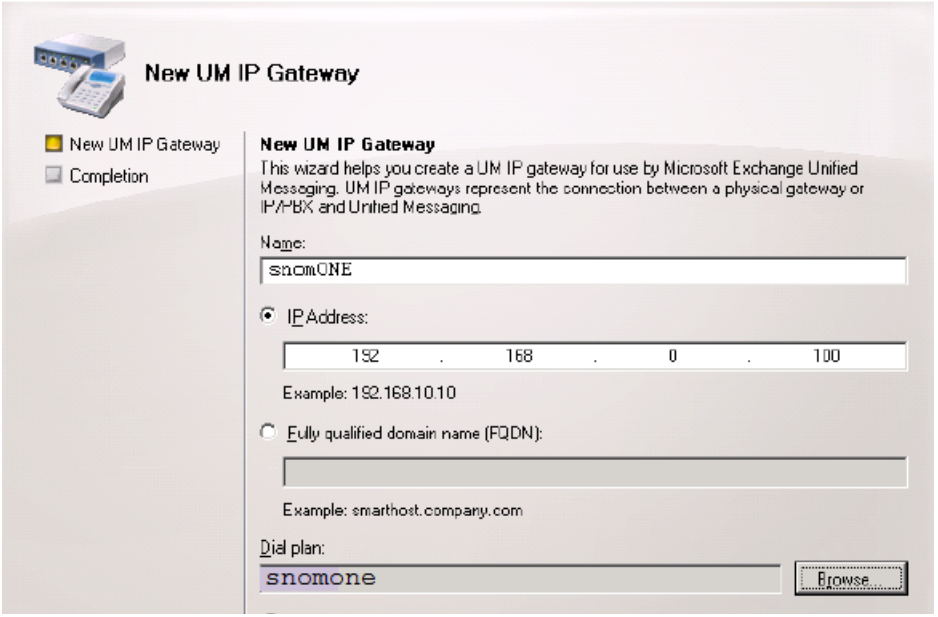
1. Install the Unified Messaging role on your Exchange 2007 Server.
2. Run Exchange Management Console. The following image displays the entries that already exist on the Exchange server.

Create a New Unified Messaging Dial Plan

1. Using the Exchange management console, select **Organization Configuration/ Unified Messaging**.
2. Under Actions, select **New UM Dial Plan**.
3. Name the dial plan `snomone`, and set the number of digits in extension numbers to `3`.
4. Click **New**, then click **Finish**.


New UM Dial Plan
New UM Dial Plan
Completion
New UM Dial Plan
This wizard helps you create a UM dial plan for use by Microsoft Exchange Unified Messaging. A dial plan is a grouping of unique telephone extension numbers.
Name:
snomone
Number of digits in extension numbers:
3

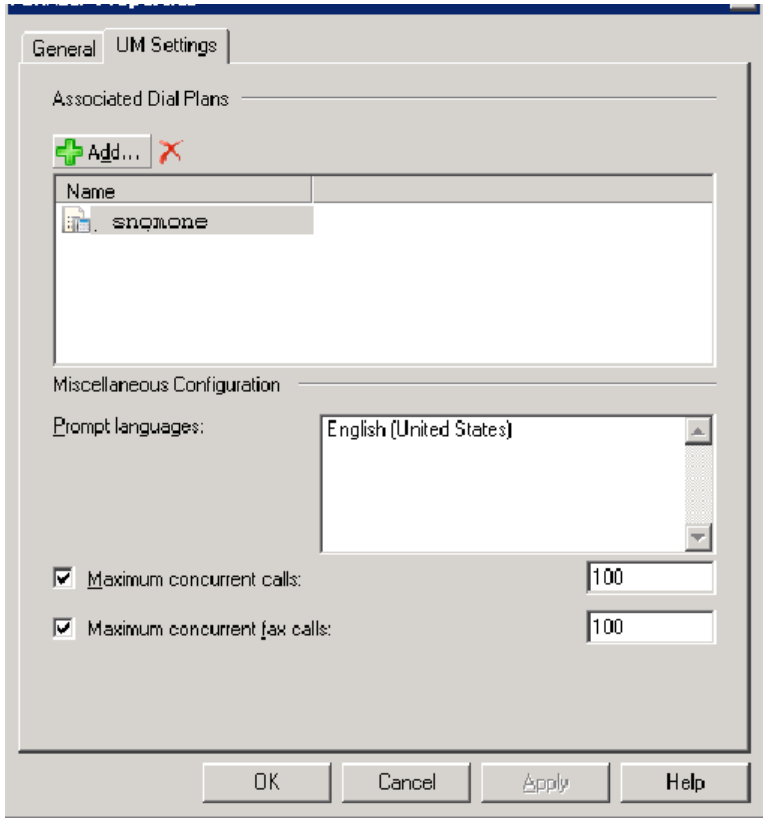
5. Create a new unified messaging IP gateway. Under Actions, select **New UM IP Gateway**. Name the gateway `snomONE`.


New UM IP Gateway
New UM IP Gateway
Completion
New UM IP Gateway
This wizard helps you create a UM IP gateway for use by Microsoft Exchange Unified Messaging. UM IP gateways represent the connection between a physical gateway or IP/PBX and Unified Messaging.
Name:
snomONE
IP Address:
192 . 168 . 0 . 100
Example: 192.168.10.10
Fully qualified domain name (FQDN):
Example: smarthost.company.com
Dial plan:
snomone
Browse...

6. Select **IP Address** and enter the IP address of your snom ONE server.
7. Click the **Browse** button, and select the `snomone` dial plan you created.
8. Click **New**, then click **Finish**.

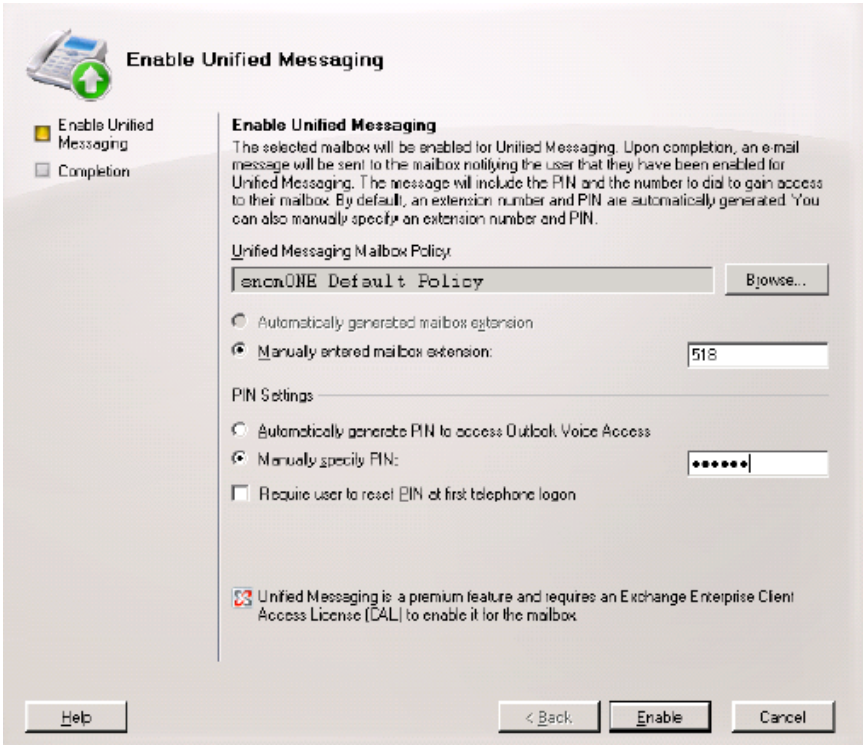
Associate the Dial Plan with the Unified Messaging Server

1. Using the Exchange management console, select **Server Configuration/Unified Messaging**. Under Actions, click **Properties** and then the **UM Settings** tab.
2. Under Associated Dial Plans, click the **Add** button.
3. Select the `snomone` dial plan you created.
4. Click **OK**.



Enable Mailbox Recipients for Unified Messaging

1. Using the Exchange management console, select **Recipient Configuration/ Mailbox**.
2. Select the mailbox you wish to enable and then under Actions, click **Enable Unified Messaging**.
3. Next to Unified Messaging Mailbox Policy, click the **Browse** button and then select **snomONE Default Policy**.
4. Enter a mailbox extension for this user that matches the user's extension number on the snom ONE server.
5. Enable **Manually specify PIN**.
6. Click **Enable**.

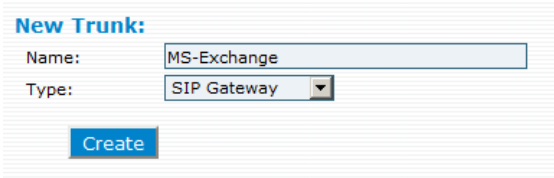

Enable Unified Messaging
Enable Unified Messaging
Completion
Enable Unified Messaging
The selected mailbox will be enabled for Unified Messaging. Upon completion, an e-mail message will be sent to the mailbox notifying the user that they have been enabled for Unified Messaging. The message will include the PIN and the number to dial to gain access to their mailbox. By default, an extension number and PIN are automatically generated. You can also manually specify an extension number and PIN.
Unified Messaging Mailbox Policy:
snomONE Default Policy
Browse...
Automatically generated mailbox extension
Manually entered mailbox extension:
518
PIN Settings
Automatically generate PIN to access Outlook Voice Access
Manually specify PIN:
Require user to reset PIN at first telephone logon
Unified Messaging is a premium feature and requires an Exchange Enterprise Client Access License (CAL) to enable it for the mailbox
Help
< Back
Enable
Cancel

7. Repeat this section for each mailbox.

Configuring the snom ONE Server

Create a new trunk to connect to Exchange:

1. Click the **Trunks** tab.
2. Name the new trunk `MS-Exchange` or any suitable name.
3. Set its type to **SIP Gateway**.



4. Click the **Create** button.
5. From the list of trunks, click `MS-Exchange`.
6. In the **Domain** field, enter the FQDN or IP address of your Exchange Server (i.e., `exchange.company.com`).
7. In the **Proxy Address** field, enter `sip:exchange.company.com:5060;transport=tcp`, but replace `exchange.company.com` with the FQDN or IP address of your Exchange Server. The example assumes the address is `100.200.100.200`.
8. Enable **Accept Redirect**.
9. If you want the PBX to do in-band DTMF to out-of-band DTMF (RFC 4733) transcoding on this trunk, set **Trunk requires out of band-DTMF tones** to **Yes**. For this to work properly, **Inband DTMF detection** must be set to on (go to **Admin** > **Settings** > **General**).
10. Click **Save**.

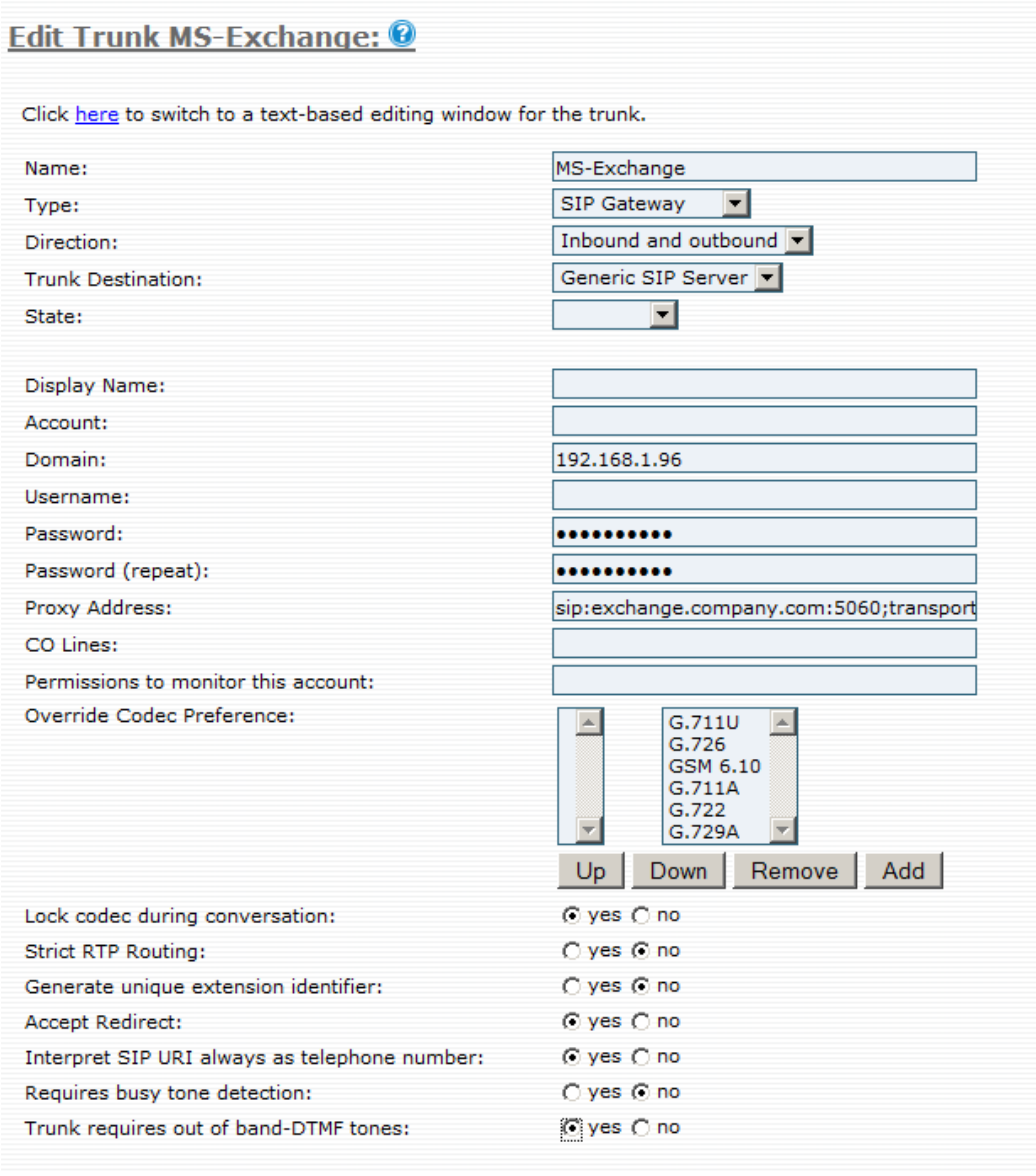
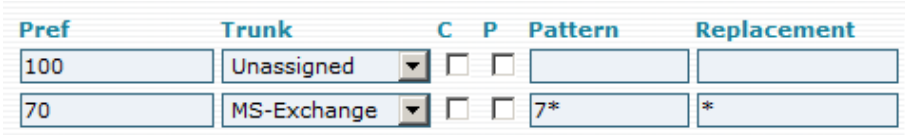


Figure C-1. Trunk Settings for Configuration with Exchange 2007/2010 UM

Add the Exchange Gateway to Your Current Dial Plan

1. From the **Dial Plans** tab, click the edit icon next to your dial plan.
2. From the dropdown in the top entry, select **MS-Exchange**.
3. Enter `7*` as the pattern and `*` as the replacement.

   Note: The digit(s) that are entered into the pattern field must match the digit(s) that were used in the **External Voicemail System** field (**Domain** > **Settings**). For example, if you used `99$u` in that field, then you can use `99*` as the pattern in the dial plan.



4. Click **Save**.

Set the snom ONE External Voicemail System

The redirection target should be a telephone number, rather than a SIP URI, and it must be possible to dial that number through the dial plan (the extension must have the permission to do that). The replacement fields known from the caller-ID representation in the trunks can be used (e.g., in the image shown below, `$u` will be replaced with the extension number). The redirection to the mailbox works only if the mailbox is enabled for that account.

1. Go to the voicemail settings in the domain, and clear the **Mailbox Direct Dial Prefix** field; otherwise, it will interfere with the mailbox redirection logic and create an endless redirection loop.

2. Set the **External Voicemail System** field as explained in the previous section.
3. Set **Offer Camp On** to **No**.
4. Click **Save**.

GLOSSARY

Address mask

A bit mask used to identify which bits in an IP address correspond to the network portion of the Internet address and which ones correspond to the subnet portions of the address. The address mask is often referred to as the subnet mask because the network portion of the address can be determined by the class inherent in an IP address. The mask is 32 bits long: ones are in positions that correspond to the network and subnet numbers, and zeros are in the host number positions.

Address resolution

The translation of an Internet address into the hardware address or IP of a network interface card (NIC). Because names are easier for people to remember, they are usually used in place of the numerical machine address to identify a piece of hardware. However, before instructions can be executed, the name must be translated into the numerical address of the hardware. This function is done by Address Resolution Protocol (see "ARP"). The terms "address resolution" and "name resolution" are synonymous.

ANI (Automatic Number Identification)

The phone number of the calling party. Used for billing and lookup purposes.

ARP (Address Resolution Protocol)

A network protocol used for determining a network host's link layer or hardware address when only its Internet layer or network layer address is known. Using the IP address of the target node, the client station broadcasts an ARP request onto the network. The node that has that address responds by sending back its physical address so that packets can be transmitted. Because ARP requests are broadcast onto the network, every station in the subnet is required to process the request. ARP returns the layer 2 address for a layer 3 address.

ATA (Analog Telephony Adapter)

A device used to connect one or more standard analog telephones to a digital and/or non-standard telephone system such as a Voice Over IP based network.

Bandwidth

The range from highest to lowest frequencies transmitted on a network. Bandwidth measures network capacity.

BLF (Busy Lamp Field)

A collection of lights or indicators on a phone that allows users to monitor the dialog state of another phone/user extension. This is indicated by the LEDs adjacent to the particular key. BLFs are often used by receptionists and secretaries to aid in routing incoming calls.

BRI (basic rate interface)

An ISDN interface that consists of two 64 kb B-channels and a 16 kb signaling channel. Defined by the ITU (International Telecommunication Union) in the I.430.

Broadcast

A transmission mode in which a station sends a message to all stations on a network. For example, an authorized user of the voicemail system might broadcast a message to all the phones on a particular domain to advise users of scheduled downtime for system maintenance.

CALEA (Communications Assistance for Law Enforcement Act)

A U. S. wiretapping law passed in 1994 to protect public safety and ensure national security. Its objective is to preserve law enforcement's ability to conduct lawfully-authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness. The law defines the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization.

CAS (content-addressed storage)

A mechanism for storing information that is in its final form (the object cannot be duplicated or modified once it has been stored). CAS assigns an identifier to the files so that they can be retrieved based on its content, rather than on their storage location. It is typically used for storing mortgage records, insurance policies, health records, and emails.

CDR (Call Detail Report)

A record produced by the system which contains the details of a call that has terminated on the system. CDRs include the date and time the call started, the number making the call, the number receiving the call, and the call duration.

Client/server

A network architecture whereby a machine is designated to serve the needs of client machines. Application services, such as file storage, network administration, and security are provided by the server to the client. Client machines are complete, standalone computers, and servers include mainframes, minicomputers, and personal computers. Client/server computing melds personal computing with centralized data processing and supports many users simultaneously.

Codecs (coder decoder)

A device used to convert binary signals transmitted on their digital networks to analog signals converted on their analog networks.

- GSM - 13 Kbps, 20ms
- iLBC - 15Kbps - 20ms & 13.3 Kbps - 30ms
- G.711 - 64 Kbps (alaw/ulaw)
- G.722 - 48/56/64 Kbps
- G.723.1 - 5.3/6.3 Kbps, 30ms frame size
- G.726 - 16/24/32/40 Kbps
- G.728 - 16 Kbps
- G.729 - 8 Kbps, 10ms
- Speed - 2.15 to 44.2 Kbps
- LPC10 - 2.5 Kbps
- DoD CELP - 4.8 Kbps

CPU (Central Processing Unit)

The central unit in a computer containing the logic circuitry that interprets and executes most of the commands from the computer's hardware and software. It is often called the "brains" of the computer, as well as the processor, microprocessor, and central processor.

DHCP (Dynamic Host Configuration Protocol)

The TCP/IP protocol for allocating IP addresses dynamically when they are needed. Devices running DHCP do not need a pre-configured IP address to join an IP-based network. As devices join the network, IP addresses are given, and as devices exit the network, IP addresses are released. DHCP is used by Internet service providers (ISPs) to allow customers to join the Internet. The DHCP protocol reduces system administration workload, allowing networks to add devices with little or no manual intervention.

DID (Direct Inward Dial)

A feature offered by telephone companies for use with their customers' private branch exchange (PBX) systems. In DID service, the telephone company provides one or more trunk lines to the customer for connection to the customer's PBX and allocates a range of telephone numbers to this line (or group of lines) and forwards all calls to such numbers via the trunk. As calls are presented to the PBX, the dialed destination number (DNIS) is transmitted, usually partially (e.g., last four digits), so that the PBX can route the call directly to the desired telephone extension within the organization without the need for an operator or attendant.

DID numbers are assigned to a communications gateway connected by a trunk to the public switched telephone network (PSTN) and the VoIP network. The gateway routes and translates calls between the two networks for the VoIP user. Calls originating in the VoIP network will appear to users on the PSTN as originating from one of the assigned DID numbers.

DISA (Direct Inward Service Access)

The process of how incoming calls are handled by a telephone system. It allows the external subscriber to make calls by dialing the extension or trunk subscriber directly without assistance of an operator. It compensates for the shortcomings of DIL and DDI.

DMZ (DeMilitarized Zone)

A computer or network zone that sits between a trusted zone (typically a LAN) and an untrusted zone (typically the Internet). A DMZ is usually separated by firewalls at each border and is used for servers (e.g., FTP) which are accessed from untrusted networks.

DND (Do Not Disturb)

A feature that prevents an extension from ringing. DND functionality allows users to silence their phones for all incoming calls, even calls made to a hunt group or an agent group, and takes precedence over call forwarding. DND can be configured with an override permission that allows a designated extension to call an extension that has been placed into DND. The DND button can be used to activate DND on a single phone; however, a user will need to activate the *78 star code so that the system will know to put the extension and any additional phone number(s) that have been configured through it into DND.

DNIS (Dialed Number Identification Service)

A telephone service that identifies for the receiver the telephone number that was dialed by the caller. Once the call enters the PBX system, the DNIS will identify which number was dialed and record that information.

DNS (domain name system)

The Internet's name/address resolution service that translates alphabetic domain names into numeric IP addresses. For example, the domain name `www.pbx.com` might translate to `198.105.232.4`. If a computer cannot access DNS, the user's web browser will not be able to find web sites and the user will not be able to receive or send email. The DNS system consists of three components: DNS data, name servers, and Internet protocols for getting the data from the servers.

Domain name server

A computer that runs a program that converts a fully qualified domain name (FQDN) into its numeric IP address and vice versa.

DTMF (Dual-Tone Multi-Frequency)

The signal that is generated when a user presses the touch keys of an ordinary telephone. Also known as "Touchtone," DTMF has essentially replaced pulse dialling. When a user presses touch keys, two tones of specific frequencies are generated (one from a high-frequency group and the other from a low-frequency group), so it's impossible for the voice to imitate the tones.

E1 (or E-1)

Similar to the North American T-1, E1 is the European format for digital transmission. E1 carries signals at 2 Mbps (32 channels at 64 kbps, with 2 channels reserved for signaling and controlling), and the T1 carries signals at 1.544 Mbps (24 channels at 64 kbps). E1 and T1 lines may be interconnected for international use.

E.164 [RFC 2916]

An international numbering plan that provides unique phone numbers worldwide. Each assigned number contains a country code (CC), a national destination code (NDC), and a subscriber number (SN). An E.164 number can be up to 15 digits. E.164 may be replaced with ENUM, which is currently being worked on by the ITU and the IETF. ENUM will encompass both traditional analog phones and digital devices, including computers and other devices on the Internet. See also "ENUM."

E911 (Enhanced 911)

A location technology advanced by the FCC that allows mobile phones to identify to emergency dispatchers the location from which a wireless call is being made. A 911 call made from a traditional phone with ground wires is routed to the nearest public safety answering point (PSAP). The PSAP receives the caller's phone number and the exact location of the phone from which the call was made and distributes the emergency call to the proper services. In contrast, 911 callers using a mobile phone had to access their service providers in order to get verification of subscription service before the call was routed to a PSAP. A 1996 FCC ruling changed this. Now a 911 call must now go directly to the PSAP without receiving verification of service from a specific cellular service provider. The call must be handled by any available service carrier even if it is not the cellular phone customer's specific carrier. The FCC rules also require that all mobile phones manufactured for sale in the United States after February 13, 2000, that are capable of operating in an analog mode, must include Enhanced 911 support. Since May 19, 2005, E911 support is required for certain VoIP service.

ENUM (Electronic NUMbering) [RFC 3761]

A protocol from the IETF that uses the domain name system (DNS) to convert a telephone number to an IP address and vice versa, enabling it to be resolved

by the Internet's DNS system like traditional Web site domains. The goal of the ENUM standard is to provide a single number to replace the multiple numbers and addresses for an individual's home phone, business phone, fax, cell phone, and e-mail.

FTP (File Transfer Protocol)

A standard Internet protocol used to upload and download files between computers that are connected to the Internet. FTP uses the Internet's TCP/IP protocols as does HTTP, which transfers displayable Web pages and related files, and SMTP, which transfers e-mail.

FQDN (fully-qualified domain name)

The complete domain name for a specific computer, or host, on the Internet. The FQDN consists of three parts: the hostname, the domain name, and the top-level domain (e.g., www.webopedia.com and sip.itsp.com).

FXO (Foreign eXchange Office) interface

A device usually found on the customer end (e.g., a plug on a phone or fax machine, or the plug on an analog phone system) that receives the analog line. Because the FXO port is attached to a device, such as a fax or phone, the device is often called an FXO device. FXO and FXS are always paired. See "FXS."

FXS (Foreign eXchange Subscriber) interface

A device usually located on the telephony company's property that sends power through a channel to a phone on the other end. It provides battery power, a dial tone, and a ring. By necessity, it must connect to an FXO device. See "FXO."

GSM (Global System for Mobile communication)

A wireless telephone standard in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA), which is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

H.323

A carrier-grade communication protocol that has been approved by the world governments as the international standard for voice, video, and data conferencing. It defines an entire, unified system for performing these functions and leverages the strengths of the IETF and ITU-T protocols.

Hub

A device for connecting one or more computers to other computers, networked devices, or to other networks. Compared to routers and switches (which are also connecting types of devices), a hub is the least complicated way to get the job done. Hubs work at the physical layer (layer 1) of the OSI model. All computers on the hub are able to see everything all the other computers on the hub see. Also see "switch" and "router."

IETF (Internet Engineering Task Force)

A body organized by the Internet Society (ISOC) that defines standard Internet operating protocols. Its mission is to produce high-quality, relevant technical documents, known as Requests for Comments (RFC), that influence the way people design, use, and manage the Internet. The IETF is supervised by the ISOC's Internet Architecture Board (IAB), and its members are drawn from ISOC's individual and organization membership. See also "ISOC."

IP-PBX (Internet Protocol Private Branch Exchange)

A telephone switch (see "PBX") located on a customer's premises that utilize VoIP to manage and deliver calls.

IPv4

A revision of Internet Protocol that uses 32 bit addressing. See also "IPv6."

IPv6

A network packet routing protocol that uses 128 bit addressing. IPv6 was developed to address the shortcomings of IPv4, such as the 32 bit address that limited the maximum number of devices that could be addressed and to extend the capabilities of IP to meet future QoS capabilities. IPv6 addresses have 8 hexadecimal numbers, separated by colons (e.g., `0800:5008:0001:0000:0002:1005:AABC:BA43`).

ISDN (Integrated Services Digital Network)

An international communications standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. ISDN supports data transfer rates of 64 Kbps (64,000 bits per second). BRI (basic rate interface) and PRI (primary rate interface) are the two types of ISDNs. The popularity of ISDN has decreased in areas where DSL and cable modem service is offered.

ISOC (Internet Society)

A nonprofit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. ISOC is supported by more than 90 organizational members and 26,000 individual members.

ITSP (Internet Telephone Service Provider)

A company that offers an Internet data service for making telephone calls using VoIP. Most ITSPs use SIP, H.323, or IAX for transmitting telephone calls as IP data packets. Customers may use VoIP phones or traditional telephones with an analog telephony adapter (ATA).

ITU (International Telecommunication Union)

A telecommunications standards body that is guided by the United Nations. It was founded as the International Telegraph Union in Paris on May 17, 1865. The ITU acts as the global focal point for governments and the private sector in developing networks and services and is comprised of more than 185 countries and produces over 200 standards recommendations annually in the areas of information technology, consumer electronics, broadcasting, and multimedia communications.

IVR (Interactive Voice Response)

A telephone technology that allows a caller to respond to configured voice menus through voice and touch tone. The IVR system responds with pre-recorded audio to further direct callers on how to proceed.

Jitter

The statistical variance of the inter-arrival times of RTP data packets. If a VoIP device sends out one RTP packet every 20 milliseconds for an audio stream, the packets will not necessarily arrive precisely every 20 milliseconds, so if the

packets are played out as they arrive, the output will produce jitter and will be of poor quality. Jitter buffers can be used to change the variable delays into constant delays.

LAN (Local Area Network)

A computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an office park. LANs are connected primarily through Ethernet and can be connected to other LANs over any distance via telephone lines and radio waves. LANs have a high data transfer rate and are not very expensive to set up. See also "WAN."

MAC (Media Access Control) address

A hardware address that uniquely identifies most network adapters or network interface cards (NICs) by the manufacturer for identification. The manufacturer's registered identification number is usually part of the MAC address if it was assigned by the manufacturer. The MAC address is used by the Media Access Control protocol sub-layer of the Data-Link Layer (DLC) of telecommunication protocols.

MIPS (million instructions per second)

An old method for measuring a computer's speed and power and, by implication, for determining the amount of work a computer can do. It measures the approximate number of machine instructions the computer can execute in 1 second (i.e., it measures CPU speed). Because there are so many variables with computer performance (e.g., varying amounts of time for different instructions, importance of I/O speed, etc.), MIPS ratings are not used that often anymore. However, a MIPS rating can give you a general idea of a computer's speed.

MoH (Music on Hold)

Recorded music that is used to fill the silence that would be heard by telephone callers who have been placed on hold.

MOS (mean opinion score)

A measurement that is used to evaluate the quality of human speech at the point of termination on any type of phone connection (audio, voice telephony, or video). A group of listeners simultaneously hear a reader recite a series of test sentences, presented by a male voice, then repeated using a female voice (computer-

generated voices are also used). The listeners individually grade the test sentences using a scale that ranges from 1 to 5 ("bad" to "excellent") and the mean score is taken. Anything below a 3 generally indicates issues with the signal processing or the bandwidth applied to the signal. Scores of 4 or 5 are usually considered stable and within industry standards, and thus acceptable.

Multicast

A network technology used for delivering information to a group of destinations at the same time. The most efficient delivery strategy is used to ensure that the messages are delivered over each link of the network only once. Copies are created only when the links to the multiple destinations split.

MWI (Message Waiting Indicator)

The red light for voicemails on a desk phone.

NAD (Network Access Device)

A device that provides access to a larger communication network (e.g., connects a LAN to a WAN). Also referred to as dialer or least cost router, a NAD reroutes calls through a network to provide the best rates for the call destination. A NAD normally includes a router, modem, and a monitored power supply. Most NADs can report power failures and reconnect themselves back to the network when disconnected.

NANPA (North American Numbering Plan Administration)

The numbering plan for the Public Switched Telephone Network for Canada, the United Stated and its territories, and the Caribbean. The plan has evolved over time into a system of three-digit area codes and seven-digit telephone numbers.

NAT (Network Address Translation or Network Address Translator)

The method for translating an IP address used within one network to a different IP address known within another network (one network is designated the *inside* network and the other is the *outside* network). NAT allows as a router, for example, to act as an agent between the public network (e.g., the Internet) and a private network (i.e., a local network), which means that a single, unique IP address can represent an entire group of computers.

NTP (Network Time Protocol) [RFC 958]

A protocol for synchronizing the clocks of computer systems using a set of distributed clients and servers. NTP uses UDP on port 123 as its transport layer and uses a jitter buffer to resist the effects of variable latency.

PBX (Private Branch eXchange)

A telephone exchange that serves a particular business or office, as opposed to one that is owned by a common carrier or telephone company and is used by many businesses or the general public. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX. PBXs have evolved over time, beginning as a manual switchboard or attendant console that was operated by a telephone operator (circuit switching) to the modern IP PBX. See also "IP PBX."

PCM (pulse code modulation)

A sampling technique that converts analog signals to digital form. The analog signal is represented by a series of pulses and non-pulses (1 or 0, respectively), and the PCM performs the analog-to-digital conversion of the speech waveform by sampling the signal 8000 times a second, encoding and transmitting the samples in a serial bit stream as 8-bit digital words. Two standards are used for coding the sample level: the U-Law standard (North America and Japan) and the A-Law standard (used in most other countries). PCM makes it possible to digitize all forms of analog data, including full-motion video, voices, music, telemetry, and virtual reality.

POTS (Plain Old Telephone Service)

The standard telephone service that most homes use. The POTS network is also called the PSTN. POTS is generally restricted to about 52 Kbps (52,000 bits per second). Non-POTS telephone services, such as ISDN and FDDI, have high-speed, digital communications lines.

Power over Ethernet (PoE)

A technology that allows the LAN switching infrastructure to provide power over a copper Ethernet cable to an endpoint or powered device. With PoE, the electrical current is not carried by power cords.

PSTN (Public Switched Telephone Network)

The network of the world's public circuit-switched telephone networks. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core and includes mobile as well as fixed (plain old telephone service, POTS) telephones. The PSTN is largely governed by technical standards created by the ITU-T, and uses E.163/E.164 telephone numbers for addressing.

PRI

A type of ISDN service designed for larger organizations. PRI service is generally transmitted through a T-1 line (or an E1 line in Europe).

Proxy Server

A server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. The VoIP proxy server is used in a DMZ of a company's secure internal communication network and receives VoIP control messages and VoIP media streams. Using the MAC address and source IP address contained in the control message, the proxy server pushes a policy change to the internal network's external firewall to open call control protocol ports and Real Time Protocol (RTP) ports only for packets from the source IP address. The VoIP proxy server hides the company's internal network address and directs incoming VoIP packets to an IP-PBX connected to the company's internal network.

QoS (Quality of Service)

A broad collection of networking technologies and techniques that are used to provide guarantees on a network's ability to deliver predictable results. In VoIP networking, quality refers to being able to listen and speak in a clear and continuous voice, without unwanted noise. When applying QoS to VoIP networks, emphasis is placed on latency (packet delivery delays), jitter (variations in packet delivery delays), packet loss (dropped packed due to too much traffic in the network), and burstiness of loss and jitter.

RAM (Random Access Memory)

A form of computer data storage that allows stored data to be accessed in any order (i.e., "random access"). RAM is used by a computer's operating system, application programs, and currently used data, so that they can quickly be reached

by the computer's processor. RAM is quickly readable and writeable compared to other kinds of computer storage (e.g., the hard disk, floppy disk, and CD-ROM); however, data in RAM remains only as long as the computer is running. Once the computer has been turned off, RAM loses its data. When the computer is turned on again, the operating system and other files are once again loaded into RAM.

RFC (Request for Comment)

A memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. RFCs are used either for peer review or to simply convey new concepts and information. The IETF adopts some of the proposals published as RFCs as Internet standards.

Router

A device for connecting one or more computers to other computers, networked devices, or to other networks. Compared to hubs and switches (which are also connecting types of devices), a router is the smartest and most complicated of the three. Routers can be programmed to understand and route the data its being asked to handle. Configuration is done through a user interface. Larger routers are capable of being programmed to communicate with other routers to determine the best method of getting network traffic from point A to point B. Hubs work at the data link and network layers (layers 2 and 3) of the OSI model.

RTCP (Real-time Transport Control Protocol) [RFC 1889, RFC 3550]

An Internet protocol used to synchronize streams (e.g., the time stamps of a video stream with the time stamps of an audio stream). RTCP works hand in hand with RTP (which does the delivery of the actual data) and sends control packets to participants in a call (in a manner scalable to large multicast networks). The primary function is to provide feedback on the quality of the data distribution being provided by RTP. See "RTP."

RTP (Real-time Transport Protocol) [RFC 1889, RFC 3550]

An Internet protocol used for transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP addresses jitter and out-of-sequence datagrams by assigning timestamps and sequence numbers to the packets. The sequence number in the RTP header enables the receiver to

put the RTP packets in order once they are received. The timestamps are used to restore the original timing relationship of the data.

SBC (session border controller)

A device used in Voice over Internet Protocol (VoIP) networks to control the signaling (and even the media streams) involved in initiating, conducting, and terminating telephone calls or other interactive media communications. Its purpose is to ease the load on the call agents within the network. A common location for an SBC is in the communication path between any two parties engaged in a VoIP session. A stand-alone SBC is often placed at a connection point, or a border, between a private local area network (LAN) and the Internet.

SDP (Session Description Protocol) [RFC 2327]

An Internet protocol that specifies how the information necessary to describe a protocol should be encoded. It includes information such as IP addresses, port numbers, and times and dates when the session is active.

SIP (Session Initiation Protocol) [RFC 3261, 3262, 3263, 3264, and 3265]

A signalling protocol for initiating and terminating an interactive user session that involves multimedia elements such as video, voice, chat, gaming, and virtual reality (it is used mainly for voice and video calls over the Internet or data networks).

SIP Trunk

A service offered by an ITSP that allows businesses that have a PBX for their internal calls to use VoIP to go outside the enterprise network by using the same connection as the Internet connection. Before SIP trunks can be deployed, a business must have a PBX with a SIP-enabled trunk side, an enterprise edge device that understands SIP, and an ITSP. See "ITSP."

SLA (Service Level Agreement)

A contract between a network service provider and a customer that details the services that the network service provider will furnish to the customer. The details of the SLA typically expand upon the services, priorities, responsibilities, guarantees, and warranties. Specifics might include the percentage of time that the service will be available, the number of users that can be served simultaneously, dial-in access availability, usage statistics, etc. The SLA allows the customer to

measure, justify, and even compare the services with those of outsourcing network providers.

SNMP (Simple Network Management Protocol) [RFC 1157]

A UDP-based network protocol used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SOAP (Simple Object Access Protocol)

An XML message-based protocol specification that allows applications running on a decentralized, distributed environment to exchange information. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other application layer protocols, such as RPT and HTTP for message negotiation and transmission. A typical example of how SOAP can be used is as follows: A SOAP message is sent to a web service enabled web site (for example, a Call Detail Record database) with the necessary parameters to populate a database. The site then returns an HTML-formatted document that includes a table taken from the database that lists the calls for the day. the requested data (prices, location, features, etc.). The data is then integrated directly into a third-party site.

Softswitch (software switch)

A term used to describe the software that is used to bridge a public switched telephone network (PSTN) and VoIP. This is done by separating the call control functions of a phone call from the media gateway (transport layer). The softswitch is typically used to control connections at the junction point between circuit and packet networks.

SRTP (Secure Real-time Transport Protocol) [RFC 3711]

A protocol that provides confidentiality, message authentication, and replay protection to Internet media traffic such as audio and video. SRTP is an extension of RTP.

STUN (Simple Traversal of UDP through NAT) [RFC 5389]

A protocol for assisting devices behind a NAT firewall or router with their packet routing. The main objective of STUN is to overcome some of the problems associated with the lack of standardized behaviors in NATs. STUN works with

a variety of NATs and application programs. However, STUN does not allow incoming UDP packets through symmetric NATs and cannot be used to obtain an Internet Protocol address (IP address) to communicate with a peer behind the same NAT.

Switch

A small device for connecting one or more computers to other computers, networked devices, or to other networks. Compared to a hub (which is also a connecting type of device), the switch is more intelligent. It is capable of picking up on traffic patterns and learning where particular addresses are. In this way, it sends traffic only where it needs to go rather than to every port, making the network significantly faster. Switches work at the data link layer (layer 2) of the OSI model.

T1 (also called channelized T1)

A digital carrier modulation method in which a T1 line is divided into 24 channels, each having a maximum data speed of 64 thousand bits per second (Kbps), and each capable of supporting a unique application that can run concurrently with, but independently of, other applications on different channels.

T.38 [RFC 3362]

A protocol that describes how to send a fax over a computer data network. T.38 allows a fax to be converted into an image and then sent to other T.38 fax devices, where it is converted back to an analog fax signal. T.38 is supported by most VoIP gateways and ATAs.

TCP (Transmission Control Protocol/Internet Protocol) [793]

The communication protocol for the Internet. TCP/IP defines the rules that computers must follow to communicate with each other over the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

TFTP (Trivial File Transfer Protocol) [RFC 1350]

A simple, less-capable form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features, so it is typically used where user authentication and directory visibility are not required (e.g., by servers to boot diskless workstations, X-terminals, and routers).

TLS (Transport Layer Security) [RFC 4346, 5246]

A protocol that ensures privacy between a client and a server. TLS authenticates both the client and the server and creates an encrypted connection between the two. TLS provides protection against eavesdropping by a third party and protection against tampering with a message. TLS is the successor to the Secure Sockets Layer (SSL).

UDP (User Datagram Protocol) [RFC 768]

A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that is using the Internet Protocol (IP). UDP merely performs IP traffic demultiplexing based on UDP port numbers, after which it provides a checksum that can be used by end systems to determine whether the datagrams received were corrupted by the network.

Unicast

The transmission method used for sending messages to a single network destination host on a packet switching network. Unicast messaging is used whenever a private or unique resource is requested.

UPnP (Universal Plug and Play)

A set of networking protocols designed to enable simple and seamless connectivity among consumer electronics, intelligent appliances, and mobile devices from many different vendors.

URI (Uniform Resource Identifier) [RFC 2396]

A string of characters for identifying all types of names and addresses on the Internet (e.g., a page of text, a video, a program, a SIP proxy). It enables devices the ability to interact with the resource over a network (typically the Internet) using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI.

Mechanism to Access Resource	Computer that Houses Resource	Name of Resource
`http://`	`www.snom.com`	`UserFiles/File1.pdf`
`https://`	`www.my-cdr-domain.com`	`cdr.php`
`sip`	`123@domain.com`	

VLAN (Virtual Local Area Network)

A software concept whereby a group of hosts with a common set of requirements communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same characteristics as a physical LAN, but end stations in a VLAN can be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VoIP (Voice over Internet Protocol)

A technology that uses Internet Protocol (IP) to transmit telephone calls over the Internet or a private internal network, rather than using circuit transmissions of the PSTN. With VoIP, the physical telephone is not necessary; users can communicate without a telephone set. A primary attraction of VoIP is its ability to reduce expenses, since telephone calls travel over the data network rather than the phone company's network.

WAN (Wide Area Network)

A computer network that covers a broad area (e.g., any network that links across metropolitan, regional, or national boundaries). WANs are similar to the Internet in that they are not owned by a single organization. They exist under collective or distributed ownership and management. For WAN connectivity over the longer distances, ATM, frame relay, and X.25 are used. Computers connected to a WAN can be connected via the telephone system, leased lines, or satellites. WANs have a lower data transfer rate when compared to LANs. See also "LAN."

XML (eXtensible Markup Language)

A flexible way to create common information formats and share both the format and the data on the Internet, intranets, etc. XML and HTML are similar, in that they both contain markup symbols to describe the contents of a page or file. However, HTML focuses on how data *looks*, whereas XML focuses on what data *is*. In HTML, text that is placed between markup tags <TITLE> and </TITLE> will simply take on the appearance (font, size, etc.) of a "title tag." However, if the same text were placed between XML markup tags <book_title> and </book_title>, it would likely mean that the data was a title of a book. Then depending on how the application in the receiving computer wanted to handle the book title, it could be stored or displayed on a website with a selection of other books that can be purchased.

INDEX

Symbols

911 95

A

access list
  blocking IP addresses 71
address book
  add agent group callers to 232
  and anonymous calls 438
  and CMC 97
  create using a CSV file 493–499
  domain address book 426
  LDAP 60
  upload address books to phone 426
  user's personal address book 422–425
administrator
  admin password 44
  admin username 44
  resetting admin password 44
  web interface for admin 30
administrator authority
  control over accounts 52
  control over ANI 52
  control over dial plans 52
  control over trunks 51
  control settings of user interface 74
agent groups 225–247, 436
  add caller to address book 232
  agents that can jump out 231
  and cell phone settings 468
  and DND 443
  feature overview 225–226
  logging in and out 244–245, 445
  message-music cycle 227–228
  monitoring 237
  naming the agent group 230
  night service 242–243
  queueing 227
  queue manager 236
  recording agent group greetings 242
  ringback in the queue 239–240
  setting up an agent group 229–243
  the From header 232
  user input handling 240
ANI 128
anonymous calls
  blocking your caller-ID 438
  rejecting using *88 439
attended transfer 433
audio
  audio__* folder 38
  audio prompts 38
  busy.wav 38
  codec preference 57
  customized ringtones 323–325
  installing new languages 321–323
  IVR language 43
  ringback.wav 38
  tone language 43
  web language 43
auto attendants 193–212
  black listed callers 198
  dial by name 197, 205
  direct destinations 205–206
  nesting auto attendants 207–209
  user input 196

welcome greetings 209–213
welcome message 193

B

black list
auto attendant 198
classify a contact 449
blind transfer 432
block anonymous calls 439
block caller-ID 438
buttons 327–341
and multiple identities 341
button functionality 328–331
button profiles 331–337
key system configuration 338–340

C

call barge 174, 445
call center
agent log in/log out 445
barging in on calls 445
listening in on calls 446
teach mode 446
call details
request using *63 star code 448
caller-ID 127, 286
and anonymous calls 439
blocking 438
unblocking 438
calling card 283–287. *See also* pre-pay
account balance 447
callback 283, 286
credit for outbound calls 98
dialing interpretation 287
DISA 283
pre-pay 283
read out balance 287
setting up the account 284–287
calling features
add to white list 448
agent log in/log out 445
black list 449
block caller-ID 438
call barge 445
call forward 439
call forward all calls 441
call forward on busy 441
call forward on no answer 442
call park 434
call pickup 435
call record 449
call return 431
call teach 446
clean up extension 448
conferencing 437
do not disturb 443
hot desking 439
intercom 431
redial 431
reject anonymous calls 439
set night mode for domain 443
show account balance 447
transer 432
wakeup call 447
call listen-in mode 446
call park
creating a park orbit account 177
park reminder 101
call park and retrieve 434

call pickup 435
call recordings
  system performance 49
call return 431
call teach 174
call teach mode 446
CDR
  CDR URL setting 47
CDR (Call Detail Record)
  midnight events 105
CDRs 393–400
  cdre, cdri, and cdrt folders 35
  global configuration file 35
  limiting the number of 46
  request call details 448
  setting a duration to keep 46
cell phones. *See also* Personal Virtual Assistant.
  and agent groups 468
  and blind transfer 432
  and conferencing 438
  and DND 443
  and hunt groups 468
  and loss-of-signal events 470
  call a cell phone without knowing number 473
  call from extension 473
  cost savings 465
  matching 95
  retrieve call from cell phone 472
  send calls to 472
  send call to cell phone 472
  specify ring schedule 468
certificates
  buying 70
  gmail SMTP server 298
  making your own 70
  size and format 70
  system certificate 68
clean up extension 448
clean up extension permission 175
CMC 97
codecs
  codec preference 57
  G.711 A-law 57
  G.711 U-law 57
  lock codec during conversation 57
  transcoding 56
conferencing 259–268
  and cell phones 438
  conference star codes 269
  participant list 266
  recording the conference 264
  the ad hoc conference 266–269
  the scheduled conference 261–262
  three-way conferencing 437
configuration files
  reload configuration files 67
  request configuration files 67
  restore/backup 66
contacts
  searching from phone display 111
  searching from web interface 111
CPU
  and agent groups 239
  limiting CDRs on system 46
  processor affinity mask 49
  setting maximum number of calls 48

CSV files 479–498
button profiles 334–335
CDR to CSV 395–396
converting Excel to CSV 486–492
domain address book 493–500
file requirements 479
required parameters 481–487
troubleshooting 501
customizing 74–80
templates 74
translation 77
user pages 78

D

dialing
dial by name 205
direct inward dialing 124–127
regular expressions 121–124
dialing settings
area code 95
CMC authentication 97
country code 94
emergency numbers 95
matching cell phone numbers 95
NANPA 94
PnP dialing scheme 107
ROW 94
dial plans 147–157
building a dial plan 153–155
configuring a CMC 148
configuring a PIN 148
preferencing 148
regular expression matching 152
replacement string 149–152
sample dial plans 155–158
wildcard patterns 151–152
DID. *See* dialing
direct destinations 205–206
disk space. *See* system performance; CPU
DND
call even if set 174
DND (do not disturb) 443
and hunt groups/agent groups 443
set using feature codes 443
domain
administering the domain 83–99
assigning an administrator 85
billing settings 97
CDR settings 97
default domain 88
domain settings 93–107
email settings 104
FQDN 84
from/to headers 96
midnight events 105
recording defaults 104
setting up a domain
area code 95
authentication user/password 108
configuring domain with ANI 95
country code 94–95
dial plan 93
dial plan scheme 107
email settings 104
emergency numbers 95
From header 96
IVR language 93
midnight events 105
music on hold 93

naming the domain 93
offering camp on 100
park reminder 101
set no-answer timeout for call forward 101
time zone 93
To header 96
tone language 93
voice mailbox settings 100
voicemail settings 98
web language 93
voicemail/mailbox settings 98
domain address book
create one with CSV file 110
downloads
audio prompts 322
MoH/paging application 385
ringtone config. file 324
snom ONE software 15
DTMF
inband 52

E

email 295–306
add email accounts 299
blacklist activity 307
blocking user interface settings 81
certificate for gmail server 298
Exchange 2007/2010 UM 531
list of conference participants 266
send call details to email account 448
send voicemails to email account 459
setting SMTP at domain level 105
SMTP server 295
system notifications 303
troubleshooting email server 62
user settings 415–418
welcome email for user 95
emergency numbers 95
Exchange 2007/2010 UM 531–537
extensions 161–173
admin-only settings 167
creating new extensions 164–167
importing bulk extensions 164
limit users who can call 175
permission settings 173–174
registration settings 169–172
restricting concurrent registrations 49
working with default extensions 162

F

file system 33–42. *See also* configuration files
directory tree 33
folder overview 35, 37–41
generated folder 370
global configuration file 34
of greetings 310
of recorded phone calls 315–320
pagmoh.xml 391
tftp folder 376
XML files 37
forwarding calls
using star codes
forward all calls 441
forward calls only when busy 441
forward calls when no answer 442
hot desking 439, 440
from/to headers 96–97

G

greetings 309–314
  agent group greetings 313–315
  auto attendant greetings 311–312
  personal greetings 309–310
  recording permission 201
  record new greetings 456
group mail 460

H

hardware
  CPU
    limiting length of voicemails 99
hot desking 439
  and agent groups/hunt groups 439
html folder 41
  customizing HTML files 36
HTTP
  logging HTTP events 62
  ports 53
hunt groups 215–222, 436
  and call pickup 436
  and cell phone settings 468
  and DND 443
  customized ringtones 222
  naming the hunt group 220
  night service 223
  permission to monitor account 223
  record incoming calls to 223
  ring stages 218, 220
  the From header 222

I

installing snom ONE
  fresh installation 5
  Linux 10
  Mac 7
  Windows 5
instant messaging 418
intercom 174, 431
IP addresses
  blocking access 71–74
IVR
  language settings 43
  logging IVR events 62
IVR node 271–282
  DTMF match list 276
  external application server 279–282
  permission to monitor account 277
  recording messages 277–278
  setting up an IVR node 274–277

L

LDAP 60
license activation 20
listen in 174
logging
  log filename 61
  logging specific events 62
  log length 61
  log messages 61
  SIP logging 63
logging in to snom ONE 19
login levels 18

M

messages

leaving a voicemail message 455
Microsoft Exchange
basic setup for Exchange Server 2007/2010 531–537
midnight events 105
reset block CID 106
reset DND flags 106
reset hotdesking 106
send daily CDR reports 105
MoH 379–391
audio_en directory 35
audio_moh folder 35
creating WAV files 383–384
mohs folder 36
setting up MoH 380
types of 379–380
monitoring
agent group manager 236
agent group queue 237
blocking monitoring settings 79
multicast
IP addresses 57
sip.mcast.net 51
music on hold. *See* MoH
MWI (message waiting indicator)
clear the MWI 462

N

NANPA 94
net start snomone 22
net stop snomone 22
night mode permission 174

P

paging 251–258
configuring paging/MoH 385–391
multicast 252
multicast IP addresses 257–258
setting up an account 253–256
unicast 251
parameters
max_tcp_length 67
ptime 57
reg_status 34
park obits
creating park orbits 177
park orbits. *See also* call park.
password
administrator login 44
password strength 45
resetting admin password 44
special password to bypass users' passwords 108
password settings
blocking on user interface 79
Personal Virtual Assistant 475
choose to offer PVA 468
PIN
compare to "Trust Caller-ID" setting 95
number of digits 99
number of digits required 99
PIN requirement 99
special PIN to override users' PINs 108
plug and play. *See* PnP
PnP 343–373
customizing pnp.xml 376
default dial plan scheme 107

DHCP 343, 344, 352–353
dial plan scheme 107
generated directory 36
generated files 370–375
logging PnP events 63
manual setup 344, 345, 355–357
mass deployment 344, 345, 354
multiple extensions on one phone 362–364
overriding PnP defaults 367–370
PnP methods 343–345
prepping the extension for 345
provisioning parameters 106–108
resetting the phone 359
SIP SUBSCRIBE 343, 344, 353–354
ports 53–57
firewalls 56
HTTP 53
LDAP 60
RTP 56
SIP 54
SNMP 58
TCP/TLS NAT refresh 50
TFTP 59
UDP NAT refresh 50
pre-pay
credit for outbound calls 98
pre-pay feature 289–294. *See also* calling card
access from calling card 294
access from extension 293
access from PVA 293
dollar amount on extension 292
rates table 290
ptimes
multicast IP addresses 58
PVA. *See* Personal Virtual Assistant.

R

record calls 449
recorded phone calls 315–320
record location setting 47
system-initiated recordings 317
user-initiated recordings 316
recordings
domain defaults 104
record hunt group calls 223
recordings folder 36, 41
redial last number called
using star codes 431
restarting the system
error file 23
Linux 22
Mac 22
Windows 21
return a call
using feature codes 431
RFC 2833 52
RFC 2976 508
RFC 3262 508
RFC 3265 508
RFC 3311 508
RFC 3428 508
RFC 3515 508
RFC 3903 508
ringback
audio_moh 35

ringing transfer 432
routing
  routing calls to extensions 119–126
ROW 94
RTP
  logging media events 62
  ports 56

S

screening calls
  anonymous calls 438
SDP
  ptime parameter 57
security
  blocking the access of IP addresses 71
service flags 181–192
  configuring a service flag 183–186
  linking flag to an account 186–189
  message/voicemail option 188–190
  night service 186–187
  permission to monitor 185
  setting the service flag 190
  using buttons with 191–192
settings
  changing hidden settings 34
SIP
  From header 96
  logging SIP events 62
  multicast 51
  ports 54
  retrieve SIP logging 65
  setting registration times 50
  short headers 51
  SIP logging 63
  To header 96
SIP overview 503–527
  CANCEL request 519
  components 504–506
  REGISTER request 516
  session establishment 513
  session termination 515
  SIP headers 526
  SIP language 507–511
  SIP response codes 528
  SIP traces 523
SNMP 58
snom ONE
  B2BUA 1
  documentation feedback 26
  downloads 15
  logging in 403
  memory requirements 2
  naming your system 42
  restarting system 16
  software installation 5
  software upgrade 20
  web interfaces 29
SOAP
  trusted IP 46
star codes
  snom ONE star codes 430
star codes (by number)
  *00 (call cell phone of extension) 473
  *51 (retrieve call from cell phone) 472
  *52 (move call to cell phone) 472
  *53 (conference) 437, 473
  *61 (show account balance) 447

*62 (wakeup call) 447
*63 (request call details) 448
*64/*65 (login/logout) 445
*66 (redial) 431
*67 (block caller-ID - activate) 438
*68 (block caller-ID - deactivate) 438
*70 (hot desking) 440
*71 (forward all calls) 441
*72 (forward all calls - deactivate) 441
*73 (forward calls on busy) 441
*74 (forward calls on busy - deactivate) 442
*75 (forward calls on no answer) 442
*76 (forward calls on no answer - deactivate) 442
*77 (transfer) 432
*78 (DND) 443
*79 (DND - deactivate) 443
*80 (set night mode) 443
*81 (call barge in) 446
*82 (call teach mode) 446
*83 (listen-in mode) 446
*84 (clean up extension) 448
*85 (call park) 434
*86 (call park retrieve) 436
*87 (call pickup) 436
*88 (block anonymous calls) 439
*89 (block anonymous calls - deactivate) 439
*90 (intercom) 431
*91 (add call to white list) 448, 449
*92 (add to black list) 449
*93/*94 (call record) 449
*95 (send voicemails to email) 459
*97 (go to voicemail) 454, 460
*98 (record new greetings) 456
*99 (clear message indicator) 462

support
online help 25
snom forum 25
snom ONE wiki 24
submitting tickets 25

symbols
yellow triangle 89

system maintenance
midnight events 105

system performance. *See also* CPU
binding pbxctrl to fixed CPU 49
call duration 50
call recordings 49
concurrent registrations 49
maximum number of calls 48
registration times 50
ring duration 50
size of backup file 49
transcoding 58
UDP and TCP/TLS NAT refresh 50

system restart
from command line 22
from Windows 21
when system fails to start 22

T

technical support
online help 24
snom forum 25
submitting tickets 25
wiki 24

TFTP
ports 59

tftp directory 42
tftp folder 36, 376
time zone
setting local time zone 43
To header
setting a new To header for the domain 96
transferring calls
attended transfer 433
blind transfer 432
from mobile device 432
transfer call to voicemail 433, 458
troubleshooting
blocked access (accesslist folder) 35
CSV files 501
midnight events 105
retrieving SIP logging 65
setting SIP logging 63
tracking system activity (logging) 60
trunks 113–144
configuring trunks 131–141
creating trunks 130
direct inward dialing (DID) 124–127
inbound calls 117–119
logging trunk events 62
outbound calls 127–130
purpose of 113–114
regular expressions 121–124
routing calls to extensions 119–126
SIP trunks 114–117

U

upgrading the software
Linux 16
Mac 16
Windows 14

V

voicemail
accessing 453
add a comment to a message 453
calling own extension 100
change your PIN 452, 453
delete a message 453
direct dial prefix 100
disk space requirements 99
envelop information 101
external voicemail system 100
fast-forward through messages 453
go straight to voicemail 460
group mail 460
leave a message 455
log in to voicemail 453
mailbox escape account 100
mailbox timeout 98
message playback 453
move or copy a message 453
no answer timeout 101
offer camp on 100
PIN - number of digits 99
PIN requirement 99
receive voicemails in email account 459
record a greeting 453, 456
record a welcome message 453
record your name 452, 453
repeat a message 453
request a callback 453
restrict length of voicemail 98
restrict number of voicemails 98
ring my cell phone when voicemail ar-

rives 470
skip a message 453
transfer call to another's voicemail 433
transfer call to your voicemail 432
voicemail prompts 38
voicemail settings
blocking from user interface 80

W

wakeup call
using star feature codes 447
WAV files
MoH 383–384
web interface
customizing the accounts page 101–103
white list
add a contact 448

How to Find Us

Berlin

snom technology AG
Charlottenstr. 68-71
10117 Berlin
info@snom.com

The entrance is at Charlottenstraße/ corner of Krausenstrasse.
Next subway station:
Stadtmitte (lines U2, U6).

Milan

snom technology SRL
Via A. Lusardi 10
IT-20122 Milano

Tel: +39 02 00611212
Fax: +39 02 93661864
info@snom.com

Paris

snom France
1er Etage Gauche
6 Parc des fontenelles
78870 Bailly

Tel: +33 1 80 87 64 87
Fax: +33 1 80 87 62 88
info@snom.com

United Kingdom

snom UK Ltd.
Aspect Court
47 Park Square East
Leeds LS12NL
United Kingdom

Tel: +441133503111
Fax: +441133503110

Boston

snom technology Inc.
18 Commerce Way, Suite 6000
Woburn, MA 01801

+1 (781) 569-2044
+1 (781) 569-2045
infoUSA@snom.com

U.S. West Coast

snom technology Inc.
910 Cloverberry Way
San Ramon, CA 94582-5575

Tel: +1 (925) 415-0170 ext 510
Fax: +1 (925) 886-2474
infoUSA@snom.com

U.S. - Miami

snom technology Inc.
11682 NW 13th MNR
Coral Springs, FL 33071

Tel: +1 978-998-7882 ext. 516
Fax: +1 978 998-7883
Cell: +1 954-614-7294
infoUSA@snom.com

Taipei

R803,5F,No.285,Sec 4,
Zhongxiao E. Rd.,
Taipei city, Taiwan ,10692

Tel: +886-2-6639-8031
Fax: +886-2-6639-8039
infoASIA@snom.com